



West Virginia Purchasing Division

2019 Washington Street, East
Charleston, WV 25305
Telephone: 304-558-2306
General Fax: 304-558-6026
Bid Fax: 304-558-3970

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: 000000100150 

SO Doc ID: LOT2400000009

Legal Name: BERRY DUNN MCNEIL & PARKER LLC


Published Date: 3/21/24

Alias/DBA:

Close Date: 3/28/24

Total Bid: \$1,598,052.00


Close Time: 13:30

Response Date: 03/28/2024 

Status: Closed

Response Time: 11:37

Solicitation Description: Network Penetration Testing and Cybersecurity Assessments

Responded By User ID: BerryDunn2 

Total of Header Attachments: 1

Total of All Attachments: 1

First Name: Ann Marie

Last Name: Lynch

Email: rfps@berrydunn.com

Phone: 2075412200

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
1	External Network Penetration Testing				283612.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments: This price includes 8 estimated assessments at \$35,451.50 per assessment.

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				208824.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments: This price includes 8 estimated assessments at \$26,103.00 per assessment.

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				546928.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments: This price includes 8 estimated assessments at \$68,366.00 per assessment.

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				558688.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments: This price includes 8 estimated assessments at \$69,836.00 per assessment.

Extended Description:

See Attached Specifications and Exhibit - A Pricing Page



PROPOSAL TO

West Virginia Lottery

TO PROVIDE

**Network Penetration Testing
and Cybersecurity
Assessments**

berrydunn.com

PROPOSAL FROM

 BerryDunn

Bill Brown, Principal
bbrown@berrydunn.com

Matt Bria, Project Manager
mbria@berrydunn.com

Proposal Due:
March 28, 2024 before 1:30 p.m.

Table of Contents



- Required CRFQ Pages..... 2**
- About BerryDunn 6**
 - Our West Virginia Relationship 6
- Security and Lottery Experience 7**
 - Governmental IT Security Expertise 7
 - Expertise in Regulatory Standards 7
 - Technology Assurance and Lottery Experience 8
- Methodology 10**
 - Planning..... 10
 - Fieldwork 11
 - External Network Penetration Testing..... 11
 - Social Engineering 11
 - Website Penetration Test..... 13
 - Internal / Client-Side Network Penetration Testing 15
 - Wireless Penetration Testing 16
 - Reporting 17
 - Proposed Work Plan 19
 - Project Assumptions..... 21
- Proposed Project Team..... 22**
 - Proposed Team Resumes 23
 - Industry Certifications..... 28
- References 31**
- Exceptions 34**
- Certificates of Insurance 35**
- Pricing Sheet 38**
- Appendix A: Sample Testing Authorization Letter 39**
- Appendix B: Requested Work Samples 42**

March 28, 2024

Brandon L. Barr, Buyer
Department of Administration, Purchasing Division
2019 Washington Street East
Charleston, WV 25305-0130

Dear Brandon Barr:

On behalf of Berry, Dunn, McNeil & Parker, LLC (BerryDunn), I am pleased to submit this proposal to the West Virginia Lottery (the Lottery) in response to the centralized request for quote (CRFQ) to provide Network Penetration Testing and Cybersecurity Assessments.

As you evaluate our proposal, please consider the following points:



We have been conducting vulnerability scanning and penetration testing for more than five years. Highly qualified and certified security auditing and security professionals comprise our engagement team. We use industry recognized best-practice techniques and methodologies to complete our penetration testing activities.



We bring extensive experience conducting risk assessments for a variety of multiprotocol and platform operating systems. BerryDunn has more than 25 years of information systems auditing and security assessment experience, including 10 years focused on serving state and local government agencies. Our team brings a deep knowledge of industry standards and frameworks, including the National Institute of Standards and Technology (NIST) Special Publications (SPs), Open Web Application Security Project (OWASP), International Organization for Standardization (ISO) 27000 series, Center for Internet Security (CIS) Top 20 Critical Controls, Payment Card Industry Data Security Standards (PCI-DSS), and other relevant standards.



We are independent and objective. We do not enter into partnerships with companies that could impair our objectivity. Not being a systems integrator or software development company allows us to make unbiased, independent recommendations. Further, BerryDunn does not partner with, consult for, or subcontract with IT systems vendors or fiscal agents. Our independence and ability to focus on your needs helps us serve as trusted advisors when needed.

As a principal of BerryDunn and the leader of our Government Assurance Practice Group, I can affirm we are committed to the contents of our proposal, and I have the authority to bind the firm to any contractual agreement resulting from this proposal. If I may clarify any information in this proposal, please do not hesitate to contact me directly.

After 50 years of assisting clients, we appreciate each new opportunity. Thank you for your time and consideration.

Sincerely,

A handwritten signature in blue ink, appearing to read 'Bill Brown'.

Bill Brown, CPA, MAFF®, CFE, Principal

t/f: 207-541-2208 | e: bbrown@berrydunn.com



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

BID RECEIVING LOCATION

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

VENDOR

Vendor Customer Code: 000000100150
Vendor Name : Berry, Dunn, McNeil & Parker, LLC
Address :
Street : 2211 Congress Street
City : Portland
State : Maine **Country :** United States **Zip :** 04102-1955
Principal Contact : William Brown Vendor Contact
Phone: 207-541-2200 **Extension:**

FOR INFORMATION CONTACT THE BUYER

Brandon L Barr
 304-558-2652
 brandon.l.barr@wv.gov

Vendor
 Signature X

FEIN# 01-0523282

DATE March 28, 2024

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

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) William Brown, Principal

(Address) 2211 Congress Street, Portland, ME 04102-1955


(Phone Number) / (Fax Number) 207-541-2200 / 207-774-2375

(email address) bbrown@berrydunn.com

CERTIFICATION AND SIGNATURE: By signing below, or submitting documentation through wvOASIS, 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.

Berry, Dunn, McNeil & Parker, LLC

(Company) 

(Signature of Authorized Representative)

William Brown, Principal / March 28, 2024

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

207-541-2200 / 207-774-2375

(Phone Number) (Fax Number)

bbrown@berrydunn.com

(Email Address)

REQUEST FOR QUOTATION
West Virginia Lottery
Network Penetration Testing and Cybersecurity Assessments

10.2. The following remedies shall be available to Agency upon default.

10.2.1. Immediate cancellation of the Contract.

10.2.2. Immediate cancellation of one or more release orders issued under this Contract.

10.2.3. Any other remedies available in law or equity.

11. MISCELLANEOUS:

11.1. Contract Manager: During its performance of this Contract, Vendor must designate and maintain a primary contract manager responsible for overseeing Vendor's responsibilities under this Contract. The Contract manager must be available during normal business hours to address any customer service or other issues related to this Contract. Vendor should list its Contract manager and his or her contact information below.

Contract Manager: William Brown
Telephone Number: 207-541-2200
Fax Number: 207-774-2375
Email Address: bbrown@berrydunn.com

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: LOT240000009

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:

(Check the box next to each addendum received)

- | | |
|--|--|
| <input checked="" type="checkbox"/> Addendum No. 1 | <input type="checkbox"/> Addendum No. 6 |
| <input type="checkbox"/> Addendum No. 2 | <input type="checkbox"/> Addendum No. 7 |
| <input type="checkbox"/> Addendum No. 3 | <input type="checkbox"/> Addendum No. 8 |
| <input type="checkbox"/> Addendum No. 4 | <input type="checkbox"/> Addendum No. 9 |
| <input type="checkbox"/> Addendum No. 5 | <input type="checkbox"/> Addendum No. 10 |

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

Berry, Dunn, McNeil & Parker, LLC

Company



Authorized Signature

3/27/2024

Date

NOTE: This addendum acknowledgment should be submitted with the bid to expedite document processing.

Revised 6/8/2012

About BerryDunn

BerryDunn is an independent consulting and certified public accounting (CPA) firm with **a dedicated team that has an extensive background conducting penetration testing and cybersecurity assessments for state, local, and quasi-governmental entities**. The services sought by the Lottery are a core strength of our firm and work we engage in every day.

We are a stable and well-established firm. BerryDunn is a privately held company that has experienced sustained growth throughout our **50-year history**, without a change in ownership. We have successfully completed numerous multiyear, high-profile engagements and have served the same clients for 5-, 10-, and 20-year durations.

Our firm provides a full range of professional services, including tax, audit, and accounting services, as well as IT, management, and financial consulting. We were formed in 1974 and have experienced sustained growth throughout our 50-year history. Today, we employ more than 875 staff members (including more than 300 in our consulting group) and serve clients nationally. BerryDunn has eight office locations across the nation:



Portland
ME



Bangor
ME



Manchester
NH



Boston
MA



Hartford
CT



Charleston
WV



Phoenix
AZ



San Juan
PR

We are proud to be a recognized leader in our industry. Now, we are the largest independently owned accounting firm headquartered in Northern New England. *Accounting Today* recently ranked BerryDunn the #1 CPA firm in New England and we are ranked #46 nationwide.

A key differentiator that BerryDunn brings is our independence from the IT systems vendor community. Our team members have many years of large-scale state and local government system implementation experience, but our firm does not sell, develop, or provide staff augmentation services for software or hardware. **This allows us to provide truly independent services, working only in the best interest of the Lottery at all times.**

Our West Virginia Relationship

West Virginia state agencies have been our clients for over 20 years. Our first contract, with the West Virginia Bureau for Medical Services (BMS), began in December 2003, and we have worked continually with BMS and other state agencies since.

BerryDunn established an office in Charleston, West Virginia, to further strengthen accessibility to our client. BerryDunn's partnership, advisement, and industry-recognized subject matter expertise remains, collaborating with and supporting West Virginia across multiple initiatives.

Security and Lottery Experience

Governmental IT Security Expertise

BerryDunn’s Government Assurance Practice Group has a team specially dedicated to IT security, as well as teams that perform internal audit risk consulting and compliance. We serve state, local, and quasi-governmental entities in all 50 states and Puerto Rico, and we have a unique understanding of government operations and the state and federal regulatory requirements with which agencies must comply. Our team is dedicated to helping government entities improve their cybersecurity profile, achieve regulatory compliance, and adopt information security programs to support organization and business objectives.

In addition to the penetration testing services the Lottery seeks, we provide the following:

Cybersecurity Maturity Development and Assessments	Regulatory Compliance Assessments (e.g., Service Organization Control, Payment Card Industry [PCI], Health Insurance Portability and Accountability Act of 1996 [HIPAA], Minimum Acceptable Risk Standards for Exchanges [MARS-E])
Incident Response and Disaster Recovery Planning	Training and Development
IT Audit and Risk Assessments	vCISO Services
Information Security Program Review and Development	Cybersecurity Capability Maturity Modeling (C2M2)
Policy Procedure Development	

Expertise in Regulatory Standards

We bring deep understanding and experience with CIS, NIST, and OWASP, as well as a range of other established standards crucial to information security and privacy, including but not limited to those illustrated in **Figure 1** below. Adhering to these guidelines helps to ensure that our assessments keep our clients current with the best security standards.

Figure 1: Industry Standards, Regulatory Guidelines, and Best Practices Used in Our Cybersecurity Assessments



We regularly perform security risk assessment activities for state and local governments, utilizing CIS Critical Controls, NIST SP 800-53, NIST Cyber Security Framework (CSF), ISO 27001, HIPAA, PCI-DSS, and other frameworks to evaluate enterprise security technology and application compliance. We assist clients with vulnerability scanning and penetration testing, internal controls reviews, regulatory requirements compliance, and establishing and improving the security and

integrity of organizational information systems. This experience includes reviewing and evaluating existing policies and procedures and developing strategic IT security roadmaps.

Our team has an in-depth knowledge of a broad range of technologies (e.g., software, hardware, and operating systems) and experience evaluating compliance with a range of security and technical standards, as shown in **Table 1**. The Lottery will benefit from BerryDunn’s knowledge and expertise in industry regulations.

Table 1: Experience with Industry Standards and Regulations

Experience with Industry Standards and Regulations
NIST Special Publication 800-115, Technical Guide to Information Security and Assessment
NIST SP 800-30 Rev.1, Guide for Conducting Risk Assessments
NIST CSF
NIST SP 800-53 Rev.4 and Rev.5, Security and Privacy Controls for Federal Information Systems & Organizations
CIS Benchmarks and Critical Security Controls
NIST SP 800-34 Rev 1, Contingency Planning Guide for Information Technology Systems
NIST SP 800-61, Computer Security Incident Handling Guide
NIST 800-144, Guidelines for Security and Privacy in Public Cloud Computing
NIST 800-145, The NIST Definition of Cloud Computing
NIST 800-146, Cloud Computing Synopsis and Recommendations

Our cybersecurity assessments consider business processes and technical requirements in the context of IT strategic goals and implementation plans. The findings and recommendations from our assessments allow our clients to establish priorities, develop meaningful action plans, and make other informed IT decisions. During our assessments, we measure how technology needs, business processes, and staff skill sets align to meet broader objectives. We look for opportunities to recommend the use of current processes, technology applications, and staffing resources, while providing recommendations that prioritize cost, productivity, and efficiency. Central to this approach, we collaborate with your stakeholders to understand your current environment.

Because this evaluation will likely result in a change in how work is currently performed, it is critical to involve stakeholders from the Lottery in the assessment process to build understanding, support, and buy-in for recommendations—and ultimately for changes in your future environment. BerryDunn’s consulting group has several certifications to provide best practices, methodologies, tools, and structure around IT governance, IT risk, IT auditing, project management, and change management to provide stability to projects making significant decisions and navigating transition.

Technology Assurance and Lottery Experience

BerryDunn’s consistently has IT and compliance related projects underway for:

- State lotteries and their major service vendors (dedicated team)
- Government and quasi-government agencies
- Colleges and universities

- Banks, fintech, and other financial organizations
- Healthcare organizations
- Other private-sector entities

We partner with our clients to assess the organizational, operational, technical, and financial aspects of their institutions to minimize risk, develop and set strategy, improve operations, streamline processes, make best use of technology and other available resources, and create innovative solutions for complex business process issues.

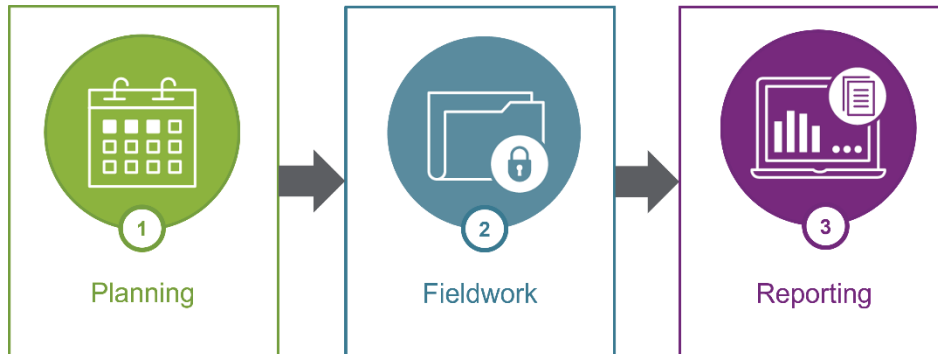
For more than 25 years, BerryDunn has been committed to working with gaming, lottery agencies, and lottery vendors across the country to assess and improve information security, financial controls, and operational processes. In the past few years, we have worked with 35 state lotteries and multiple lotteries in Canada and Europe, either directly or through their major service providers. We have significant experience working as independent and objective auditors for IGT Global Solutions Corporation (IGT) and Scientific Games, LLC (SG). We have also worked with the NorthStar Lottery in both New Jersey and Illinois. We are knowledgeable of all aspects of these vendors' operations, and because of this, we can provide the Division with integrated performance audits, based on scope, of both the Lottery and their key vendors.

We are committed to the success of the lottery industry. As of February 2024, we are currently the only CPA firm who is an associate member of the North American State and Provincial Lottery Association (NASPL). We attend NASPL's annual conferences, and members of our team have spoken at the annual Professional Development Seminars on emerging audit and security topics for the last five years.

Methodology

BerryDunn has a proven approach to conducting the services requested by the Lottery. We propose a three-phased work plan, outlined below, to conduct the required testing and assessments.

Figure 2: Project Phases



Our methodologies for conducting each specific type of testing the Lottery requires, as well as our reporting process, are discussed in detail below. If at any time during the testing BerryDunn identifies a critical vulnerability, is able to gain privileged access, or gains access to sensitive data, we will immediately notify the designated Lottery staff member to discuss approved steps to proceed with the test.

Planning

Project planning will begin upon acceptance of our proposal and successful negotiation of a contract. Based on existing documentation, terms of the contract, as well as input from project leadership and project stakeholders, will be determined. Our proposed project team will be led by Matt Bria, a senior manager who is a certified Project Management Professional® (PMP®) and Certified Information Systems Security Professional (CISSP). Our project management approach is derived from established and proven methodologies and best practices as defined by the Project Management Institute® (PMI®). Project management best practices form the foundation for all of our project efforts and provide a proven framework for BerryDunn’s execution of this project. Throughout the engagement, BerryDunn will conduct status meetings and provide status reports on a weekly interval.

During this phase, BerryDunn will facilitate an initial kickoff meeting with the Lottery project team and stakeholders. We will introduce the BerryDunn team, review BerryDunn’s testing methodology, discuss the scope of penetration testing assessment, review project assumptions, and further refine dates and/or tasks.

Based on our discussions in the project kickoff meeting and other communications, we will customize the project plan into a detailed plan and schedule that best meets the needs of the Lottery. Additional planning meetings will be scheduled to refine the scope of the penetration tests. During these meetings, we will identify assets such as web applications and Internet Protocol (IP) ranges that will be included in the scope of each test. At the conclusion of these meetings, BerryDunn will develop Rules of Engagement (ROE) for the penetration testing efforts. The ROE will define the scope, methodology, communication channels, and timelines for the penetration testing

efforts. The ROE will include the Tactics, Techniques and Procedures (TTPs) and tools to be utilized during testing. Further, an Authorization Letter wherein the Lottery provides BerryDunn written approval to conduct network penetration testing is required prior to any testing activities. BerryDunn will provide the Lottery with a copy of our Authorization Letter (a sample of which is included in **Error! Reference source not found.**), which needs to be reviewed and signed prior to commencing the penetration testing efforts.

Fieldwork

External Network Penetration Testing

During the mutually agreed-upon dates and times, as defined within the ROE, BerryDunn will perform external penetration testing, emulating a threat actor. BerryDunn will utilize a commercial vulnerability scanner, QualysGuard—as well as Kali-Linux-based, open-source tools—to scan all in-scope components to determine ports, protocols, and services running on each component. BerryDunn will begin with a network discovery scan that sweeps the agreed-upon IP address ranges, polling a set of common transmission control protocol (TCP)/user datagram protocol (UDP) ports and services, as well as sending various Internet Control Message Protocols (ICMP) probes. The purpose of this enumeration scan will be to discover responding hosts within the IP address space and confirm client understanding of services exposed to the internet. It will also enable the identification of any additional candidate hosts (web applications) to receive a full vulnerability assessment via our enterprise scanning devices.

The network scan will efficiently determine all operating systems and services that are running and available on the network. The BerryDunn vulnerability scanner includes high-speed checks for more than 3,000 of the most commonly updated vulnerabilities and a wide variety of scanning options for every network setup.

Exploitation: Exploitation will use a testing process that systematically exploits identified vulnerabilities in selected systems. Each test is customized for the target system and may include a number of attack techniques. We will use publicly-available exploitation code, commercial penetration testing tools, and proprietary exploitation techniques to help ensure the thoroughness of testing and reduce false positives.

Post Exploitation: If access is achieved, we will attempt to gain escalated privileges to find additional vulnerabilities, gather detailed system information, or move laterally within the in-scope networked environment. Evidence of such information will be limited to screenshots and the placement of flags when possible. BerryDunn will not attempt to exfiltrate data from the environment.

Social Engineering

This form of penetration testing assesses the awareness employees have about protecting the corporate network. BerryDunn will attempt to manipulate employees into providing access to a network or system which can then be leveraged into elevated access. BerryDunn may two types of social engineering testing:

- **Logical:** BerryDunn utilizes targeted emails (*phishing*) that request network access information or installs hidden malware when the user clicks on a link in an email or an SMS

text. Extended testing includes providing “free” or innocuous-looking USB drives that install malware that will allow the testers to fully access the user’s PC.

- *Verbal:* Utilizing phone calls (*vishing*) and conversations, BerryDunn will attempt to elicit network access information. Once that information is obtained, the next step is to use that information to elevate the user’s privileges to an administrative level.

We are committed to meeting the requirements listed in **Section 4.1 of the CRFQ, Mandatory Requirements for External Network Penetration Testing**. All remote system scanning, and attempts to exploit vulnerabilities or escalate privileges are conducted with proper care to avoid any disruption of service

External Network Penetration Testing Requirements per Section 4.1 of the CRFQ	Status
External Network Penetration Testing may be performed remotely.	✓
Time frames, testing schedule, target completion dates and exclusions will be documented within the ROE.	✓
<p>A four-phased structure methodology, including reconnaissance, mapping, discovery, and exploitation will be followed.</p> <ul style="list-style-type: none"> • Reconnaissance to include: <ul style="list-style-type: none"> ○ Perform WHOIS, ARIN, and DNS (public server) lookups ○ OSINT – Public Searches/Dorks ○ Build custom password lists ○ DNS lookups (entities server) ○ Gather information from entities network resources ○ Analyze metadata • Mapping to include: <ul style="list-style-type: none"> ○ Network Discovery (ICMP sweeps, traceroutes, bypass firewall restrictions, etc.) ○ Port/Protocol Scanning (Scan for accepted IP protocols, open TCP/UDP ports) ○ OS/Version Scanning (Identify underlying OS and software and their versions) • Discovery to include: <ul style="list-style-type: none"> ○ Vulnerability Scanning (Identify vulnerabilities. Open source tools as well as Commercial: Nessus – network vulnerability scanner, Burp Suite – web application scanner) ○ Enumerating Network Services (Connect and interact with services to disclose information, gain access, identify misconfigurations, etc.) ○ Username/Email Enumeration (Validate and guess usernames/emails using login forms, network services, etc.) 	✓
Must identify exploitable vulnerabilities and demonstrate organizational impact.	✓
Denial of service (DoS) attacks are prohibited for External Network Penetration Testing services.	✓
A social engineering exercise must be included. This will consist of a single phishing email scenario targeting approximately 200 active Lottery staff. The content must be designed to	✓

External Network Penetration Testing Requirements per Section 4.1 of the CRFQ	Status
maximize successful phishing, and the email content and target addresses must be verified and approved by the Lottery.	
Heavy load brute force or automated attacks will only be performed with prior Lottery approval.	✓
Must notify Lottery of any portion or portions of the assessment resulting in service disruption.	✓
The Lottery must be notified immediately upon identifying any security vulnerability threatening critical business processes or IT services.	✓

Website Penetration Test

During the mutually-agreed-upon dates and times defined within the ROE, the test team will perform vulnerability scans and penetration testing on agreed-upon internet-accessible IP ranges. BerryDunn will utilize a commercial web application scanner, Qualys—as well as Kali-Linux-based, open-source tools such as Zed Attack Proxy (ZAP)—to scan all in-scope web applications. Utilizing the results gained from the web application scans, the project team will attempt to exploit identified vulnerabilities and obtain access to protected information. This test assesses how well the security controls protect assets from a direct attack. The BerryDunn team proposes that web application testing to be conducted from both unauthorized/unauthenticated and authorized/authenticated users’ perspectives

We are committed to meeting the requirements listed in **Section 4.2 of the CRFQ, Mandatory Requirements for Website Penetration Testing**. All remote system scanning, and attempts to exploit vulnerabilities or escalate privileges are conducted with proper care to avoid any disruption of service. Brute-force or denial of service testing will not be performed without explicit approval and coordination with the Lottery.

Website Penetration Testing Requirements per Section 4.2 of the CRFQ	Status
Website Penetration Testing may be performed remotely.	✓
Timeframes, testing schedule, target completion dates and exclusions will be documented within the ROE.	✓
Identification of static and dynamic page counts.	✓
Any environment, such as production, development, quality assurance, etc., may be tested. Each environment will be assessed separately.	✓
<p>A four-phased structure methodology, including reconnaissance, mapping, discovery, and exploitation.</p> <ul style="list-style-type: none"> • Reconnaissance to include: <ul style="list-style-type: none"> ○ Perform WHOIS, ARIN, and DNS (public server) lookups ○ OSINT – Public Searches/Dorks ○ Build custom password lists 	✓

Website Penetration Testing Requirements per Section 4.2 of the CRFQ	Status
<ul style="list-style-type: none"> ○ DNS lookups (entities server) ○ Gather information from entities web applications ○ Analyze metadata ● Mapping to include: <ul style="list-style-type: none"> ○ SSL/TLS Analysis (Identify accepted SSL/TLS ciphers) ○ Virtual Hosting and Load Balancer Analysis ○ Software Configuration Discovery (Identify HTTP version, web services, scripting languages, third-party web applications, etc.) ○ HTTP Options Discovery (Identify accepted HTTP methods) ○ Web Application Spidering (Gather/follow all links) ○ Directory Browsing (Identify web directory listings, brute force common web directory names) ○ Web Application Flow (Identify the business logic, flow, organization, and functionalities of the app) ○ Session Analysis (Identify locations where session cookies are set and analyze predictability) ● Discovery to include: <ul style="list-style-type: none"> ○ Vulnerability Scanning (Identify vulnerabilities. Open source tools as well as Commercial: Nessus – network vulnerability scanner, Burp Suite – web application scanner) ○ Username/Email Enumeration (Validate and guess usernames/emails using login forms, network services, etc.) ○ Identify Web Application Specific/Web Service Specific Vulnerabilities (Command/XML/XXE/SQL Injection, File Inclusion, Directory Traversal, File Upload, XSS, CSRF, etc.) ○ Identify Authentication/Authorization Issues/Bypasses (Weak access control, weak password policy, session management, etc.) ● Exploitation to include: <ul style="list-style-type: none"> ○ Brute Force Logins (Using discovered username/email addresses, gain additional access through brute force) ○ Exploitation (Using discovered vulnerability information, exploit vulnerabilities to gain additional access/disclose information) ○ Post-Exploitation and Pivot (Pillage the system to disclose information and additional vulnerabilities. Repeat the penetration test steps to attempt to gain privileged access. Use the compromised systems as a pivot point to attack other systems that are in scope) 	
DoS attacks are required for Website Penetration Testing and require notification to the Lottery and Lottery approval before the attack commences.	✓
Heavy load brute force or automated attacks will only be performed with prior Lottery approval.	✓

Website Penetration Testing Requirements per Section 4.2 of the CRFQ	Status
Identification of website vulnerabilities exist by testing each website, including server operating systems, application platforms, and databases.	✓

Internal / Client-Side Network Penetration Testing

The BerryDunn team will attempt to sniff and capture network traffic to identify network assets, ports, and protocols that may allow for lateral movement across the network. BerryDunn will attempt to exploit vulnerable services and applications to gain initial system access as well as attempt to escalate privileges using techniques such as pass-the-hash, password spraying, password cracking and by searching for credentials in documents stored in files systems and shares. BerryDunn will attempt to locate and identify sensitive information residing on systems. Further, if agreed upon within the ROE, an attempt to exfiltrate data may be made.

The internal testing is designed to test the Lottery’s ability to detect malicious activity and help ensure events and systems are properly being monitored. During all testing activities, we recommend that the Lottery monitor its network defenses (firewalls, security incident and event management, intrusion detection system/intrusion prevention system [IDS/IPS]) to assess the effectiveness of those systems in detecting and alerting personnel of an attack. Because such systems are difficult to configure and maintain, this type of testing is an opportunity to test the systems’ effectiveness.

We are committed to meeting the requirements listed in **Section 4.3 of the CRFQ, Mandatory Requirements for Internal / Client Side Network Penetration Testing**. All remote and on-site system scanning and attempts to exploit vulnerabilities or escalate privileges are conducted with proper care to avoid any disruption of service.

Internal / Client-Side Network Penetration Testing Requirements per Section 4.3 of the CRFQ	Status
Internal/Client Side Network Penetration Testing must be performed on-site at all Lottery locations. Assessing locations remotely or from one central location is prohibited.	✓
Time frames, testing schedule, target completion dates and exclusions will be documented within the ROE.	✓
<p>A four-phased structure methodology, including reconnaissance, mapping, discovery, and exploitation will be followed:</p> <ul style="list-style-type: none"> • Reconnaissance to include: <ul style="list-style-type: none"> ○ Identification of software versions along with potentially useful software configurations or settings ○ Identification of any anti-malware, firewall, and IDS products on the system ○ Gathering of information about the network (i.e., domain user/group information, domain computers, password policy) ○ Verification of the ability to execute scripts or third-party programs • Mapping and Discovery to include: 	✓

Internal / Client-Side Network Penetration Testing Requirements per Section 4.3 of the CRFQ	Status
<ul style="list-style-type: none"> ○ Identification of vulnerabilities affecting the provided host ○ Determining the possibility of receiving and executing various malicious payloads ● Exploitation to include: <ul style="list-style-type: none"> ○ Attempts to bypass anti-malware solutions and security restrictions, escape restricted environments, and escalate privileges ○ Using discovered vulnerability information, exploit vulnerabilities to gain additional access/disclose information 	
Testing shall assess the security of all networked assets, including but not limited to servers, endpoints, firewalls, network devices, and network monitoring and management.	✓

Wireless Penetration Testing

Wireless penetration testing begins with network scans that sweep the IP address ranges provided within the technical test plan, polling a large set of TCP/UDP ports and services, and also sending various ICMP probes. The purpose of this enumeration scan is to discover responding wireless hosts and access points within the IP address space and identify systems that are operating in the environment. BerryDunn will also scan for rogue WAPs within the identified facilities (locations). Reconnaissance will attempt to determine the following: names of broadcasting and non-broadcasting service set identifiers (SSIDs), use of encryption, types of protocols in use (a/b/g/n), number of communications channels being used, and the model and vendor of equipment.

Capturing packets on wireless networks is an efficient way to determine types and sources of traffic that are running on the Lottery’s WAPs. These captures will also provide details about the types and levels of encryption being used at each access point.

We are committed to meeting the requirements listed in **Section 4.4 of the CRFQ, Mandatory Requirements for Internal / Client Side Network Penetration Testing**. All remote and on-site system scanning and attempts to exploit vulnerabilities or escalate privileges are conducted with proper care to avoid any disruption of service.

Wireless Penetration Testing Requirements per Section 4.4 of the CRFQ	Status
Wireless Penetration Testing must be performed on-site at all Lottery locations. Assessing locations remotely or from one central location is prohibited.	✓
Timeframes, testing schedule, target completion dates and exclusions will be documented within the agreed upon ROE.	✓
A four-phased structure methodology, including reconnaissance, mapping, discovery, and exploitation will be followed: <ul style="list-style-type: none"> ● Reconnaissance to include: <ul style="list-style-type: none"> ○ Perform WHOIS, ARIN, and DNS (public server) lookups ○ OSINT – Public Searches/Dorks ○ Build custom password lists ○ DNS lookups (entities server) 	✓

Wireless Penetration Testing Requirements per Section 4.4 of the CRFQ	Status
<ul style="list-style-type: none"> ○ Gather information from entities web applications ○ Analyze metadata ● Mapping to include: <ul style="list-style-type: none"> ○ Sniffing (establishing a baseline of traffic, sniff Wi-Fi, Bluetooth, Zigbee, and other RF) ○ War Walk (map location of access points and their coverage, identify leakage) ○ Identify Rogue Access Points* (Friendly, malicious, or unintended access points) ● Discovery to include: <ul style="list-style-type: none"> ○ Identification of Points of Attack (Identify WEP networks, capture WPA/WPA2 PSK key exchanges, identify clients for evil-twin and MiTM attacks) ○ Enumerating Services (Connect and interact with services on APs, Bluetooth Devices, and other RF devices to disclose misconfigurations) ○ Vulnerability Scanning (Identify vulnerabilities) ● Exploitation to include: <ul style="list-style-type: none"> ○ AP Attacks (Exploit hotspots, perform MiTM attacks, crack WEP, crack WPA/WPA2 PSK, etc.) ○ Client Attacks (Perform Evil-Twin attacks, perform rogue AP attacks, MiTM, etc.) ○ Denial of Service where applicable and with prior Lottery approval ○ Bluetooth/Zigbee/SDR Attacks where applicable and with prior Lottery approval 	
Testing to assess the security of all wireless assets.	✓

Reporting

For each of the penetration testing categories (External Network Penetration Testing, Website Penetration Testing, Internal/Client-Side Network Penetration Testing, and Wireless Penetration Testing), an Executive Summary and Technical Report will be provided. The Executive Summary report will be directed to the senior management level and will provide for an overview of the test results, scope, approach, findings, and recommendations. The Technical Report will contain level of detail needed for the technical support teams to address identified weaknesses and vulnerabilities. The Technical Report will also include detailed test methodology, strengths, weaknesses, detailed findings, risk rating, recommendations, and supporting vulnerability details. All reports will be provided to the Lottery in a secure electronic method.

Reporting Requirements per section 4.1 through 4.4	Status
<p>External Network Penetration Test</p> <ul style="list-style-type: none"> ● Executive Summary Report to include: <ul style="list-style-type: none"> ○ An overview of all testing results, including a summary report of the scope and approach, findings, key points of strength in the assessed infrastructure, and recommendations directed at senior management ● Technical Report to include: 	✓

Reporting Requirements per section 4.1 through 4.4	Status
<ul style="list-style-type: none"> ○ Details each vulnerability type discovered along with a critical, high, medium, or low risk rating ○ How the vulnerability was discovered ○ The potential impact of its exploitation ○ Recommendations for remediation ○ Vulnerability references 	
<p>Website Penetration Test</p> <ul style="list-style-type: none"> ● Executive Summary Report <ul style="list-style-type: none"> ○ An overview of all testing results, including a summary report of the scope and approach, findings, key points of strength in the assessed infrastructure, and recommendations directed at senior management ● Technical Report to include: <ul style="list-style-type: none"> ○ Details each vulnerability type discovered along with a critical, high, medium, or low risk rating ○ How the vulnerability was discovered ○ The potential impact of its exploitation ○ Recommendations for remediation ○ Vulnerability references 	✓
<p>Internal/Client-Side Penetration Test</p> <ul style="list-style-type: none"> ● Executive Summary Report <ul style="list-style-type: none"> ○ An overview of all testing results, including a summary report of the scope and approach, findings, key points of strength in the assessed infrastructure, and recommendations directed at senior management ● Technical Report to include: <ul style="list-style-type: none"> ○ Details each vulnerability type discovered along with a critical, high, medium, or low risk rating ○ How the vulnerability was discovered ○ The potential impact of its exploitation ○ Recommendations for remediation ○ Vulnerability references 	✓
<p>Wireless Penetration Test</p> <ul style="list-style-type: none"> ● Executive Summary Report <ul style="list-style-type: none"> ○ An overview of all testing results, including a summary report of the scope and approach, findings, key points of strength in the assessed infrastructure, and recommendations directed at senior management ● Technical Report to include: <ul style="list-style-type: none"> ○ Details each vulnerability type discovered along with a critical, high, medium, or low risk rating ○ How the vulnerability was discovered ○ The potential impact of its exploitation ○ Recommendations for remediation ○ Vulnerability references 	✓

Additionally, an on-site or web meeting will be conducted with the Lottery team to present the findings, strengths, weaknesses, and vulnerabilities identified during the test. Both the Executive Report and Technical Report will be developed to align with the reporting requirements defined within sections 4.1 through 4.4 of the CRFQ.

Proposed Work Plan

Below is a detailed outline of our work plan to complete each penetration test category. Each testing category approach will be customized based on your needs. BerryDunn strives to be flexible when it comes to developing and executing an effective project plan. We understand that no two projects are exactly alike and believe that one of the primary reasons we have been successful with similar projects is our willingness to be flexible in adapting to our clients' unique needs.



Phase 1: Planning

Transparency, effective communication, and adequate planning are key factors to a successful engagement.

Task	Description
1.1	Schedule project kickoff meeting Introductory meeting between BerryDunn project manager and Lottery project manager.
1.2	Conduct project kickoff meeting Kickoff meeting with team members and stakeholders from BerryDunn and the Lottery.
1.3	Conduct detailed planning meetings Detailed scoping meetings between BerryDunn testing team and Lottery technical team(s).
1.4	Develop Penetration Testing Plan and Schedule Project work plan and schedule to be approved by the Lottery before testing begins.
1.5	Develop and prepare Rules of Engagement (ROE) document Defines the steps to be taken and the tools and equipment to be used to facilitate testing, as well as the information to be collected and submitted in the final report.
1.6	Prepare and sign Letter of Authorization Provides BerryDunn with written approval to conduct the testing.
Deliverables D1: Rules of Engagement (ROE) document D2: Letter of Authorization D3: Penetration Testing Plan for Lottery Review and Approval Additional: Weekly Status Reports (throughout engagement)	



Phase 2: Fieldwork

Appropriate stakeholder engagement will help increase support and minimize potential resistance to any changes that result from our assessment.

Task	Description
2.1	Perform Reconnaissance Gathering and collection of network assets and footprint.
2.2	Perform Mapping Mapping of network, identification of ports, services, operating systems.
2.3	Perform Discovery Vulnerability scanning and enumeration of services.
2.4	Perform Exploitation Exploitation testing of identified vulnerabilities and gaps in security posture.
Deliverable: Additional: Weekly Status Reports (throughout engagement)	



Phase 3: Reporting

We adhere to stringent quality management and control standards to help ensure deliverables and reports are timely, accurate, and of the highest quality.

Task	Description
3.1	Complete gap analysis of all testing and assessments BerryDunn analysis of test results.
3.2	Develop and provide Executive Summary and Technical Report BerryDunn team develops the two reports and delivers to the Lottery.
3.3	Deliver Findings Presentation In-person or web meeting to provide the Lottery team with strengths, weaknesses, and vulnerabilities identified during the testing.
Deliverable: D4: Executive Summary Report D5: Technical Report	

Project Assumptions

BerryDunn made several assumptions in the development of our approach, determination of team composition, and estimate of the hours and cost required to complete the scope of work for this project. Should any of these assumptions be inaccurate, we would be happy to discuss them with the Lottery and adjust our proposed approach accordingly to achieve the desired project results. Our assumptions are as follows:

- These projects are a priority for the Lottery. The relevant entities for each assessment will make resources available for key informant interviews as requested and respond to requests for information promptly.
- The project will receive commitment and support from management and project stakeholders. The Lottery will designate a senior-level individual who will be authorized during the term of each project to act as the project's primary contact. This individual must have the authority to make decisions about actions to be taken by BerryDunn and on behalf of the relevant entity.
- The work plan, including detailed tasks, subtasks, timelines, and involved stakeholders, will be refined with you during the initial project planning phase.
- Project phases may not all occur in a sequential manner (i.e., activities in one phase may overlap activities in another phase to minimize the impact on stakeholders and maximize efficiencies).
- The Lottery acknowledges and agrees that if any responsibility as set forth in the CRFQ and proposal is not performed by the Lottery, then BerryDunn will be relieved of providing the affected BerryDunn services to the extent the nonperformance impacts BerryDunn's ability to provide affected services.
- The Lottery acknowledges that significant changes in the scope may result in additional costs and extension of the project timeline.
- The appropriate stakeholders review each draft and submit feedback to BerryDunn within 10 business days.
- References to days or weeks refer to working days rather than total days. Working days are defined as Monday through Friday, not including federally recognized holidays. For example, "30 days" would equal approximately 35 consecutive calendar days.
- The designated project manager for each assessment will assist in the coordination of planning meetings.
- The Lottery will provide advance notice if you cannot meet the agreed-upon deliverable review timelines.
- The contract monitor will assist with risk mitigation and issue resolution as needed to help keep the project on track.

Proposed Project Team

BerryDunn carefully selects team members for our project work based on their strengths, project experience, subject matter expertise, industry knowledge, certifications, and education. Our team is structured to provide the most effective service for a proposed project. BerryDunn currently employs 21 dedicated security consultants.

BerryDunn's proposed team members are committed to serving their clients' needs. While we do not anticipate needing to replace project team members, we believe it is important that the Lottery understands we have qualified resources to step in if needed. Should the need arise to replace key personnel on a project, we will notify your project manager of this need in writing and provide the opportunity to approve replacements. In the event we need to draw upon backup personnel, we have developed processes and systems to provide all project team members with the information they need to understand the project's history and quickly get up to speed on the project status.

Our experience working with state and local governments has shown that a team approach provides projects maximum value by offering the deep experience of a principal, the specialized skills of an engagement/project manager, and the technical and administrative skills of subject matter experts (SMEs) and supporting staff, all in a cost-conscious manner. On the following pages, we have included resumes for our proposed team members for the Lottery's projects.

Proposed Team Resumes



Bill Brown, CPA, MAFF®, CFE

Principal

Bill is the principal leading BerryDunn's Government Assurance Practice Group, bringing 35 years of audit, cost accounting, financial consulting, compliance assessment, and management consulting experience. He oversees performance and

IT audit engagements for state and local governments as well as program integrity, fraud, and risk audits. With a focus on financial management, compliance and risk management, and information security, he takes a personal approach to serving each client's specific needs and implementing tools and strategies to help them minimize their risk profile and improve their regulatory and financial stability.

Relevant Experience

Security Assessments: Bill has served as the project principal for security assessments for client systems such as eligibility and enrollment systems, data warehouses, claims systems, databases, government servers, water department systems, asset management systems, and wireless networks.

Independent Security Assessments: Bill has led multiple security assessments for government clients, utilizing the NIST SP 800 Series, Minimum Acceptable Risk Standards for Exchanges (MARS-E) (v2.0), IRS 1075, the Affordable Care Act (ACA), and HIPAA. Assessment activities include review of policies and procedures, vulnerability scanning and penetration testing, and configuration assessments of servers and databases.

PCI Assessments: Bill oversees BerryDunn's team that provides PCI security and gap assessments, which include mapping out each client's cardholder data environment (CDE), providing guidance on policies and procedures, performing a PCI gap analysis, and developing a PCI security program to help ensure the security of credit card data.

Program and Compliance Audits: Bill has led program audits and compliance assessments for numerous clients. These engagements include assessments of internal controls, policies and procedures, financial activities, and accounts; document reviews and interviews; audit readiness assessments; program requirements compliance; IT general controls and applications examinations; and process reviews.

Past Clients

City and County of Denver, CO Auditor's Office
City of Malden, MA
City of Philadelphia, PA
City of Phoenix, AZ
City of Scottsdale, AZ
Colorado Office of the State Auditor
Larimer County, CO
Maricopa County, AZ Internal Auditor's Department
Metropolitan Government of Nashville Davidson County, TN
Minnesota Information Technology Services
New Hampshire Liquor Commission
New Hampshire Secretary of State
Puerto Rico Medicaid Program

Education and Certifications

BS, Accounting, University of Southern Maine
Certified Public Accountant
Master Analyst in Financial Forensics®
Certified Fraud Examiner

Memberships

National Association of Certified Valuators and Analysts
Association of Certified Fraud Examiners



Matt Bria, CISSP, PMP®, GSNA, PCI-QSA, Prosci® CCP

Senior Manager –

Matt is a senior manager in BerryDunn's Government Assurance Practice Group and leads BerryDunn's IT Security Practice. He leads several of BerryDunn's IT security engagements, including security maturity

assessments and information security program development. He possesses a strong knowledge and understanding of security analytics, enterprise resource planning security, network and cloud security, security architecture, security governance, risk assessments, and compliance. Matt is a certified Project Management Professional® (PMP®), Certified Information Systems Security Professional (CISSP), GIAC Systems and Network Auditor (GSNA), and PCI-QSA with 19 years of security-related project management experience.

Key Qualifications

- National Institute of Standards and Technology (NIST) and MARS-E
- NIST CSF
- Security Program Development
- Security Maturity
- Incident Response and Ransomware Readiness

Relevant Experience

Security Assessments and Program Development: Matt has served as the project manager for security assessments for client systems such as eligibility and enrollment systems, data warehouses, claims systems, databases, government servers, water department systems, asset management systems, and wireless networks. Matt is well-versed in security frameworks such as NIST 800-53, NIST Cybersecurity Framework (CSF) assessment framework, CIS, and MARS-E. Matt has led security assessments, security maturity assessments, and security program development projects for cities such as Nashville, TN; Phoenix, AZ; Scottsdale, AZ; Fate, TX; Maricopa County, AZ; Larimer County, CO; and Glynn County, GA. Additionally, Matt has led security assessments for state-based agencies in Puerto Rico, New Mexico, Missouri; Minnesota; West Virginia; and Indiana.

Director of IT Security: Prior to joining BerryDunn, Matt served as the IT Security Director for TBC Corporation. He was responsible for all aspects of enterprise-wide security and enterprise production change management for a multi-billion dollar retail and wholesale organization. He had direct management of a team responsible for enterprise security architecture, identity and access management, intrusion detection and analysis, multi-factor authentication, advanced malware detection, security analytics, forensics, DLP, incident response, and endpoint protection.

Past Clients

City of Phoenix, AZ
City of Scottsdale, AZ
City of Fate, TX
Metropolitan Government of Nashville Davidson County, TN
Glynn County, GA
Larimer County, CO
Maricopa County, FL
Pasco County, FL
Indiana Department of Family and Social Services
Minnesota Information Technology Services
Missouri Department of Social Services
New Mexico Health Insurance Exchange
Puerto Rico Medicaid Program
West Virginia Department of Health and Human Resources

Education and Certifications

BS, Management Information Systems, Salve Regina University
Certified Information Systems Security Professional (CISSP)
Project Management Institute® Certified Project Management Professional® (PMP®)
GIAC Systems and Network Auditor (GSNA)
Payment Card Industry Qualified Security Assessor (PCI-QSA)
Prosci® Certified Change Practitioner (CCP)



Mitch Darrow, GPEN

Manager

Mitch is a manager with 25 years of experience in business system analysis, database design, system architecture, network administration, and design engineering. He has provided leadership on technology projects to measure, analyze, and

improve performance issues, training and development, project coordination, as well as strategy and planning for information technology projects related to human services. He joined BerryDunn in 2014 after 14 years with Sappi Fine Paper North America.

Relevant Experience

Penetration Testing and Vulnerability Scanning: Mitch specializes in providing clients with penetration testing and vulnerability scanning services. Clients include Columbia College, Indiana Department of Family and Social Services, West Virginia Department of Health and Human Resources, Puerto Rico Department of Health and Human Services, New Mexico Health Insurance Exchange, Missouri Department of Social Services, and Minnesota Department of Employment and Economic Development.

Independent Security Assessments: Mitch works on multiple security assessments for government clients, utilizing the NIST SP 800 Series, MARS-E (v2.0), IRS 1075, the Affordable Care Act (ACA), and HIPAA. Assessment activities include review of policies and procedures, and configuration assessments of servers and databases.

Past Clients

Alaska Division of Legislative Audit
City of Philadelphia, PA
City of Phoenix, AZ
City of Scottsdale, AZ
Colorado Department of Human Services
Columbia College
Glynn County, GA
Indiana Department of Family and Social Services
Metropolitan Government of Nashville Davidson County, TN
Minnesota Department of Employment and Economic Development
Minnesota Information Technology Services
Missouri Department of Social Services
New Mexico Health Insurance Exchange
Puerto Rico Department of Health and Human Services
Sacramento Municipal Utility District
West Virginia Department of Health and Human Resources

Education and Certifications

BS, Mechanical Engineering, Iowa State University
GIACC Certified Penetration Tester (GPEN)
Proficiency in several programming languages, including Visual Basic, VB Script, PowerShell, and XSLT



Louis Krupp, CISSP, GSNA, PCI-QSA

Senior Consultant

Louis is a senior consultant with BerryDunn's Government Assurance Practice Area, focusing on information technology (IT) security projects. Louis brings a passion for penetration testing and vulnerability scanning to determine and reduce business risk. He has an intermediate level of programming experience, aiding in development of custom scripts used to gather and assess system and database configurations using scripting languages such as PowerShell and bash. He has previous experience using other languages, including Java, C++, C# SQL, HTML, ASP, and VB Script. He is currently completing a Penetration Testing with Kali Linux course to get his Offensive Security Certified Penetration Tester certification.

Key Qualifications

- Experience with local and state-based clients
- Proficient in analyzing security controls and frameworks
- Experience analyzing and interpreting of system configurations, vulnerability scanning, and application scanning results
- Experience reviewing technical documentation, including policies, procedures, and plans

Relevant Experience

Security Assessments: Louis is well-versed in security frameworks such as NIST 800-53, NIST Cybersecurity Framework (CSF) assessment framework, CIS, and MARS-E. Louis has served as a lead security analyst for security assessments, security maturity assessments, and security program development projects for City's such as Nashville, TN; Phoenix, AZ; Scottsdale, AZ; Maricopa County, AZ; Larimer County, CO; and Glynn County, GA. Additionally, Louis has performed security assessments for state-based agencies in Alaska, Puerto Rico, New Mexico, Missouri; Minnesota; West Virginia; and Indiana.

Penetration Testing and Vulnerability Scanning: Louis has provided penetration testing and vulnerability scanning services for clients including the Metropolitan Government of Nashville Davidson County and Columbia College.

Program Audits: Louis has served as a security subject matter expert for audits of government programs across the country, including assisting the Minnesota Department of Labor and Industry with their Workers' Compensation Modernization Program system audit; the Alaska Division of Legislative Audit with the examination of their IT general and application controls; and the West Virginia Department of Health and Human Resources with their Medicaid EHR Provider Incentive Program audit.

Past Clients

Alaska Division of Legislative Audit
City of Phoenix, AZ
City of Scottsdale, AZ
Glynn County, GA
Larimer County, CO
Maricopa County, AZ
Metropolitan Government of Nashville Davidson County, TN
Minnesota Department of Employment and Economic Development
Minnesota Department of Labor and Industry
Minnesota Information Technology Services
Missouri Department of Social Services
New Mexico Health Insurance Exchange
Ohio School Employees Retirement System
Puerto Rico Department of Health and Human Services
Puerto Rico Medicaid Program

Education and Certifications

BS, Computer Science and Security and Cyber Defense, Thomas College
Certified Information Systems Security Professional (CISSP)
GIAC Systems and Network Auditor (GSNA)
Payment Card Industry Qualified Security Assessor (PCI-QSA)



Spencer Treece

Consultant

Spencer is a cybersecurity consultant in BerryDunn's Government Assurance Practice Group. He thrives on remediating challenges presented during security research and system architecture assembly. He possesses a passion for problem solving and learning, as

well as the discipline required to ensure top-tier work is delivered to clients in pursuit of maturing their security posture and assuring their security controls. He is a determined leader with a strong knowledge and understanding of security analytics and architecture, application security, network and cloud security, vulnerability scanning, risk assessment, and compliance. He brings an iron-clad work ethic, an unwavering attention to detail, and a quenchless need for excellence to any work he approaches. As a consultant with the Government Assurance Practice Group, Spencer has been responsible for conducting managerial policy and procedure review against the National Institute of Standards and Technology (NIST) SP 800-53 and MARS-E standards, as well as assisting with risk assessments regarding the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Key Qualifications

- Risk Assessment
- Vulnerability Scanning
- National Institute of Standards and Technology (NIST) and MARS-E
- Network and Traffic Analysis
- System Architecture

Relevant Experience

MARS-E Assessments: Using the CMS MARS-E assessment framework, Spencer has performed MARS-E assessments for the Puerto Rico Medicaid Program and the New Mexico Health Insurance Exchange.

Security Assessments: Spencer has participated in security and risk assessments for the Indiana Family and Social Services Administration's Bureau of Disabilities web application. He keeps his skills sharp pursuing assessment-related industry certifications, featuring hands-on experience with simulated real-world assets.

Past Clients

Puerto Rico Medicaid Program

New Mexico Health Insurance Exchange

Indiana Family and Social Services Administration

Education and Certifications

AA, Culinary Arts with Honors, The Illinois Institute of Art

CompTIA Security+

CompTIA Network+

Splunk Core Certified User

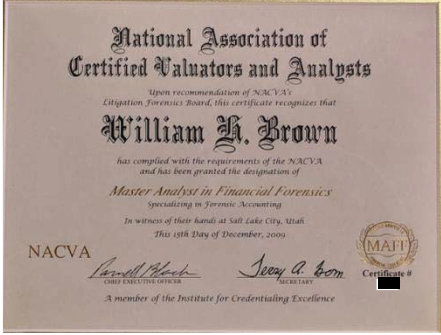
Microsoft Azure Fundamentals

Industry Certifications

Proposed team leaders hold a variety of licenses and certifications that will benefit the Lottery. Mitch Darrow possesses a GPEN certification, demonstrating his high level of expertise and familiarity with the tactics of cyber intruders. Matt Bria is a certified Project Management Professional® (PMP®) who offers a sophisticated approach to the management of projects such as this one.

In **Table 2**, we have provided the professional certifications currently held by the members of our project team as requested in the Lottery’s CRFQ. These certifications are backed by nationally recognized industry associations and boards, further reflecting the dedication and knowledge they bring to the Lottery.

Table 2: Professional Certifications

Team Member	Certifications
<p style="writing-mode: vertical-rl; transform: rotate(180deg);">Bill Brown, CPA, MAFF®, CFE</p>	<div style="display: flex; justify-content: space-between;"> <div style="width: 48%;">  <p>State of Maine DEPARTMENT OF PROFESSIONAL AND FINANCIAL REGULATION OFFICE OF PROFESSIONAL AND OCCUPATIONAL REGULATION BOARD OF ACCOUNTANCY</p> <p>License Number [REDACTED]</p> <p>Be it known that WILLIAM H. BROWN has qualified as required by Title 32 MRS Chapter 113 and is licensed as: CERTIFIED PUBLIC ACCOUNTANT</p> <p>Issue Date: August 1, 2023 Expiration Date: September 30, 2024 Commissioner: Anne L. Head</p> </div> <div style="width: 48%; text-align: center;">  <p>CERTIFIED FRAUD EXAMINER</p> <p>William H. Brown, CFE, CPA Member # [REDACTED] Certified: February 19, 2010 Expiration Date: August 31, 2024</p> </div> </div> <div style="margin-top: 10px;">  <p>National Association of Certified Valuers and Analysts Upon recommendation of NACVA's Litigation Forensics Board, this certificate recognizes that William H. Brown has complied with the requirements of the NACVA and has been granted the designation of Master Analyst in Financial Forensics specializing in Forensic Accounting. In witness of their hand at Salt Lake City, Utah This 15th Day of December, 2009</p> <p>NACVA Certificate # [REDACTED]</p> </div>

Team Member	Certifications
-------------	----------------

**Matthew Bria, PCI-QSA, CISSP, PMP®, GSNA, Prosci®
CCP**

Mitch Darrow, GPEN

Team Member	Certifications
Louis Krupp, PCI-QSA, CISSP, GSNA	  

References

To demonstrate BerryDunn’s relevant experience and the quality of our past work, on the following pages we have provided reference information for three clients for whom we have performed similar projects. The client representatives listed can speak to our expertise, proven methodology, and effective project communications.

Reference 1	
Customer Name	Metropolitan Government of Nashville and Davidson County (Metro), TN
Contact Person	John Griffey Information Systems Assistant Director 700 2nd Avenue South Nashville, TN 37219
Email Address	john.griffey@nashville.gov
Telephone Number	615-880-2786
Description	<p>BerryDunn is assisting in the development of the Information Security Management Program for the Metropolitan Government of Nashville and Davidson County (the Metro). BerryDunn has been tasked with completing the following objectives:</p> <ul style="list-style-type: none"> • Information Security Program development and management • Information risk management and compliance • Aid in the development of an IT-focused risk management program, including processes and procedures for: <ul style="list-style-type: none"> ○ Risk identification, assessment, and evaluation, including the creation of a risk register and development of risk scenarios ○ Risk response, including processes for performing a cost-benefit analysis to aid in determining appropriate responses ○ Risk monitoring and reporting, including development of risk-based metrics ○ Information security incident response plan management <p>In addition to the work performed in developing the Information Security Management Program, BerryDunn has also completed security assessments for Metro’s Sheriff’s and Water Departments. BerryDunn has also provided Metro with PCI advisory and Qualified Security Assessor (QSA) assessment activities.</p>

Reference 2	
Customer Name	City of Phoenix, AZ Audit Department
Contact Person	Aaron Cook Deputy City Auditor – IT 17 S. 2 nd Avenue, #200 Phoenix, AZ 85003
Email Address	aaron.cook@phoenix.gov
Telephone Number	602-495-6985
Description	<p>BerryDunn conducted an assessment to evaluate the City of Phoenix's (Phoenix's) standards and operating procedures that pertain to the configuration and patch management processes for Phoenix's database and server infrastructure. The assessment focused on the following core areas:</p> <ul style="list-style-type: none"> • Database: Administration; User Access Security; Configuration and Parameter Settings; Logging and Monitoring; Availability, Backup, and Recovery • Server: Governance; User Access Security; Configuration and Parameter Settings; Logging and Monitoring <p>BerryDunn evaluated controls based on NIST SP 800-53, the Internal Revenue Service (IRS) Office of Safeguards Computer Security Evaluation Matrix (SCSEM) and CIS benchmarks.</p> <p>BerryDunn randomly selected a subset of databases and servers to perform assessment against. The sample size was based on best practice calculations defined by the American Institute of Certified Public Accountants (AICPA).</p> <p>Over the course of the assessment, BerryDunn evaluated over 235 databases, covering varying types such as DB2, Oracle 11g and 12c and SQL 2008,2012, 2014 and 2016. An additional 1,100+ virtual servers, virtual machine (VM) hosts, and vCenters were analyzed covering Windows and various Linux versions.</p> <p>Additionally, BerryDunn conducted on-site interviews with Phoenix's various technical support team and reviewed Phoenix's policies and procedures.</p> <p>At the conclusion of the project, BerryDunn provided Phoenix with three distinct deliverables</p> <ul style="list-style-type: none"> • Database Assessment Report • Assessment Report • Project Closeout Report

Reference 3	
Customer Name	City of Scottsdale, AZ City Auditor's Office
Contact Person	Lai Cluff Senior Auditor 7447 E. Indian School Rd., Suite 205 Scottsdale, AZ 85251
Email Address	lcluff@scottsdaleaz.gov
Telephone Number	480-312-7851
Description	<p>The Scottsdale, Arizona, City Auditors office engaged with BerryDunn to perform an audit to evaluate the enterprise wireless network. To evaluate the security of the enterprise wireless network, BerryDunn performed the following activities:</p> <ul style="list-style-type: none"> • Wireless Governance and Management Review • Network administrators and security team interviews • Wireless network vulnerability assessment • Wireless vulnerability and risk analysis <p>The primary objective of the audit was to assess the adequacy of IT security controls that are in place for the City's enterprise wireless network. BerryDunn conducted a vulnerability assessment of the enterprise wireless network and evaluated security controls pertaining to:</p> <ul style="list-style-type: none"> • Wireless network architecture • Encryption • Configuration Management • Access Management • Monitoring <p>BerryDunn assessed the City's implementation of the enterprise wireless network. The enterprise wireless network was defined as wireless networks service set identifiers (SSID's) that are centrally managed by the City's IT department. Enterprise wireless networks were present in 22 locations across the City, with some locations having multiple SSIDs. At each location visited, BerryDunn performed scans to identify rogue access points that may be broadcasting and attempted to exploit weakness of the enterprise wireless network.</p>

Exceptions

Listed below are two requested exceptions to the Lottery's provided terms and conditions. We believe in being fully transparent about any potential conflicts at the time of proposal. To this end, we have our Compliance Team perform a thorough review. As consultants focused on government clients, we are well aware of the limitations on exceptions and additional constraints. If selected for this project, we fully expect to work with the Lottery to reach an agreement on these terms that is fair and beneficial to both parties.

CRFQ, General Terms and Conditions, Section 19 (p. 16) – We would like to request that written notice and an opportunity to cure be provided before the Contract is terminated for cause as in Section 19.

CRFQ, General Terms and Conditions, Section 36 (p. 19) – BerryDunn has a robust professional liability insurance policy for acts or omissions of BerryDunn, our agents, employees, and subcontractors. This policy contains language within it that states that it will not apply if BerryDunn takes on additional liabilities under contract, such as the agreement to indemnify a party for its own negligence, or a third party's negligence. In order to help ensure that our clients have the protection of this policy as requested in this CRFQ, we ask to clarify that the indemnification language attaches to situations where BerryDunn has failed to perform its obligations under contract. Our preferred language is: "The Vendor agrees, to the fullest extent permitted by law, to indemnify and hold harmless the Agency against damages, liabilities, and costs arising from the negligent acts of the Vendor in the performance of professional services under this Agreement, to the extent that the Consultant is responsible for such damages, liabilities, and costs on a comparative basis of fault and responsibility between the Vendor and Agency."

Certificates of Insurance



CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY)
06/13/23

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER Affinity Insurance Services 1100 Virginia Drive, Suite 250 Fort Washington, PA 19034	CONTACT NAME: PHONE (A/C, No, Ext): _____ FAX (A/C, No): _____ E-MAIL ADDRESS: _____ INSURER(S) AFFORDING COVERAGE INSURER A : Columbia Casualty Company NAIC # 31127 INSURER B : _____ INSURER C : _____ INSURER D : _____ INSURER E : _____ INSURER F : _____
INSURED Berry, Dunn, McNeil & Parker, LLC 2211 Congress Street Portland, ME 04102	

COVERAGES **CERTIFICATE NUMBER:** **REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS
	COMMERCIAL GENERAL LIABILITY <input type="checkbox"/> CLAIMS-MADE <input type="checkbox"/> OCCUR GEN'L AGGREGATE LIMIT APPLIES PER: <input type="checkbox"/> POLICY <input type="checkbox"/> PRO-JECT <input type="checkbox"/> LOC. <input type="checkbox"/> OTHER: _____						EACH OCCURRENCE \$ DAMAGE TO RENTED PREMISES (Ea occurrence) \$ MED EXP (Any one person) \$ PERSONAL & ADV INJURY \$ GENERAL AGGREGATE \$ PRODUCTS - COMPI/OP AGG \$ _____ \$
	AUTOMOBILE LIABILITY <input type="checkbox"/> ANY AUTO <input type="checkbox"/> OWNED AUTOS ONLY <input type="checkbox"/> SCHEDULED AUTOS <input type="checkbox"/> HIRED AUTOS ONLY <input type="checkbox"/> NON-OWNED AUTOS ONLY						COMBINED SINGLE LIMIT (Ea accident) \$ BODILY INJURY (Per person) \$ BODILY INJURY (Per accident) \$ PROPERTY DAMAGE (Per accident) \$ _____ \$
	UMBRELLA LIAB <input type="checkbox"/> OCCUR EXCESS LIAB <input type="checkbox"/> CLAIMS-MADE DED RETENTION \$						EACH OCCURRENCE \$ AGGREGATE \$ _____ \$
	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) <input type="checkbox"/> Y <input type="checkbox"/> N <input type="checkbox"/> A If yes, describe under DESCRIPTION OF OPERATIONS below						PER STATUTE OTH-ER E.L. EACH ACCIDENT \$ E.L. DISEASE - EA EMPLOYEE \$ E.L. DISEASE - POLICY LIMIT \$
A	Media, Network Security, Privacy Liability			652108915	05/31/2023	05/31/2024	Aggregate Limit \$10,000,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

CERTIFICATE HOLDER Berry, Dunn, McNeil & Parker, LLC 2211 Congress Street Portland, ME 04102	CANCELLATION SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS. AUTHORIZED REPRESENTATIVE
--	--

© 1988-2015 ACORD CORPORATION. All rights reserved.

ACORD 25 (2016/03)

The ACORD name and logo are registered marks of ACORD



CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY)
05/23/2023

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

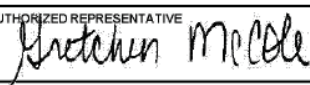
PRODUCER Affinity Insurance Services 1100 Virginia Drive, Suite 250 Fort Washington, PA 19034	CONTACT NAME: Gretchen McCole PHONE (A/C, No, Ext): 215-773-4600 FAX (A/C, No): E-MAIL ADDRESS: gretchen.mccole@aon.com
	INSURER(S) AFFORDING COVERAGE NAIC # INSURER A : Continental Casualty Company 20443 INSURER B : Evanston Insurance Company 35378 INSURER C : INSURER D : INSURER E : INSURER F :
INSURED Berry, Dunn, McNeil & Parker, LLC 2211 Congress Street Portland, ME 04102	

COVERAGES **CERTIFICATE NUMBER:** **REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS
	COMMERCIAL GENERAL LIABILITY <input type="checkbox"/> CLAIMS-MADE <input type="checkbox"/> OCCUR GEN'L AGGREGATE LIMIT APPLIES PER: <input type="checkbox"/> POLICY <input type="checkbox"/> PRO-JECT <input type="checkbox"/> LOC OTHER:						EACH OCCURRENCE \$ DAMAGE TO RENTED PREMISES (Ea occurrence) \$ MED EXP (Any one person) \$ PERSONAL & ADV INJURY \$ GENERAL AGGREGATE \$ PRODUCTS - COMP/OP AGG \$ \$
	AUTOMOBILE LIABILITY <input type="checkbox"/> ANY AUTO <input type="checkbox"/> OWNED AUTOS ONLY <input type="checkbox"/> SCHEDULED AUTOS <input type="checkbox"/> HIRED AUTOS ONLY <input type="checkbox"/> NON-OWNED AUTOS ONLY <input type="checkbox"/> AUTOS ONLY						COMBINED SINGLE LIMIT (Ea accident) \$ BODILY INJURY (Per person) \$ BODILY INJURY (Per accident) \$ PROPERTY DAMAGE (Per accident) \$ \$
	UMBRELLA LIAB <input type="checkbox"/> OCCUR EXCESS LIAB <input type="checkbox"/> CLAIMS-MADE DED RETENTION \$						EACH OCCURRENCE \$ AGGREGATE \$ \$
	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below						<input type="checkbox"/> PER STATUTE <input type="checkbox"/> OTH-ER E.L. EACH ACCIDENT \$ E.L. DISEASE - EA EMPLOYEE \$ E.L. DISEASE - POLICY LIMIT \$
A	Professional Liability			APL-188112791	04/01/2023	04/01/2024	Per Claim/Aggregate Limit \$5,000,000 / \$5,000,000
B	Excess Professional Liability			MKL7XE0000169	04/01/2023	04/01/2024	Per Claim/Aggregate Limit \$5,000,000 / \$5,000,000 SIR applies per policy terms and conditions.

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

CERTIFICATE HOLDER Berry Dunn McNeil & Parker, LLC 2211 Congress Street Portland, ME 04102	CANCELLATION SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS. AUTHORIZED REPRESENTATIVE 
--	--

© 1988-2015 ACORD CORPORATION. All rights reserved.

ACORD 25 (2016/03)

The ACORD name and logo are registered marks of ACORD



BERRDUN-03

HCTALBOT

CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY)
4/25/2023

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER Clark Insurance 1945 Congress Street, Bldg A PO Box 3543 Portland, ME 04104-3543	CONTACT NAME: Heather Caston-Talbot, AAI, CIIP, CIC	
	PHONE (A/C, No, Ext):	FAX (A/C, No):
	E-MAIL ADDRESS: hcaston-talbot@clarkinsurance.com	
	INSURER(S) AFFORDING COVERAGE	
	INSURER A : Hanover American	NAIC # 36064
	INSURER B : Massachusetts Bay	22306
	INSURER C : The Hanover Insurance Company	22292
	INSURER D : Maine Employers Mutual Ins Co	11149
	INSURER E : Travelers Property Casualty Co. of America	25674
	INSURER F :	

INSURED
Berry Dunn McNeil & Parker LLC
PO Box 1100
Attn: Jodi Coffee
Portland, ME 04104

COVERAGES CERTIFICATE NUMBER: REVISION NUMBER:

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADD'L INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS
A	<input checked="" type="checkbox"/> COMMERCIAL GENERAL LIABILITY <input type="checkbox"/> CLAIMS-MADE <input checked="" type="checkbox"/> OCCUR <input checked="" type="checkbox"/> ISO form CG 00 01 GEN'L AGGREGATE LIMIT APPLIES PER: <input type="checkbox"/> POLICY <input checked="" type="checkbox"/> PROJECT <input checked="" type="checkbox"/> LOC OTHER:			ZZP D240054	4/30/2023	4/30/2024	EACH OCCURRENCE \$ 1,000,000 DAMAGE TO RENTED PREMISES (Ea occurrence) \$ 1,000,000 MED EXP (Any one person) \$ 15,000 PERSONAL & ADV INJURY \$ 1,000,000 GENERAL AGGREGATE \$ 2,000,000 PRODUCTS - COMP/OP AGG \$ 2,000,000
B	AUTOMOBILE LIABILITY <input type="checkbox"/> ANY AUTO OWNED AUTOS ONLY <input checked="" type="checkbox"/> HIRED AUTOS ONLY <input type="checkbox"/> SCHEDULED AUTOS <input checked="" type="checkbox"/> NON-OWNED AUTOS ONLY			ADPD240058	4/30/2023	4/30/2024	COMBINED SINGLE LIMIT (Ea accident) \$ 1,000,000 BODILY INJURY (Per person) \$ BODILY INJURY (Per accident) \$ PROPERTY DAMAGE (Per accident) \$ Hired Auto P.D. \$ 50,000
C	<input checked="" type="checkbox"/> UMBRELLA LIAB <input checked="" type="checkbox"/> OCCUR <input type="checkbox"/> EXCESS LIAB <input type="checkbox"/> CLAIMS-MADE DED <input checked="" type="checkbox"/> RETENTION \$ 0			UHP D240055	4/30/2023	4/30/2024	EACH OCCURRENCE \$ 8,000,000 AGGREGATE \$ 8,000,000
D	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below Y / N <input checked="" type="checkbox"/> N / A			5101800149	1/1/2023	1/1/2024	<input checked="" type="checkbox"/> PER STATUTE <input type="checkbox"/> OTH-ER E.L. EACH ACCIDENT \$ 1,000,000 E.L. DISEASE - EA EMPLOYEE \$ 1,000,000 E.L. DISEASE - POLICY LIMIT \$ 1,000,000
E	Employee Theft			105608076	4/30/2023	4/30/2024	Limit 5,000,000
E	Employee Theft			105608076	4/30/2023	4/30/2024	Of Client Prop Limit 5,000,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)
 30 day notice of cancellation with 10 days notice for non-payment of premium, if required by written contract/agreement.

CERTIFICATE HOLDER Berry Dunn McNeil & Parker 2211 Congress Street Portland, ME 04102	CANCELLATION SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.
	AUTHORIZED REPRESENTATIVE

ACORD 25 (2016/03)

© 1988-2015 ACORD CORPORATION. All rights reserved.

The ACORD name and logo are registered marks of ACORD

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	\$ 35,451.50	\$ 283,612.00
2	4.2	Website Penetration Testing	8	\$ 26,103.00	\$ 208,824.00
3	4.3	Internal/Client-Side Network Penetration Testing	8	\$ 68,366.00	\$ 546,928.00
4	4.4	Wireless Penetration Testing	8	\$ 69,836.00	\$ 558,688.00
TOTAL BID AMOUNT					\$ 1,598,052.00

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:	Berry, Dunn, McNeil & Parker, LLC
Vendor Address:	2211 Congress Street, Portland, ME 04102
Email Address:	bbrown@berrydunn.com
Phone Number:	207-541-2200
Fax Number:	207-774-2375
Signature and Date:	March 28, 2024

Appendix A: Sample Testing Authorization Letter

On the following pages, we have included a sample of our testing authorization letter.

Security Testing Authorization Letter

Berry, Dunn, McNeil & Parker LLC., (BerryDunn) has been contracted to perform security testing (which may include vulnerability testing, web application testing and penetration testing) on the <client name>'s computer network (inclusive of all systems and assets connected to that network as identified by <client name>).

The purpose of this letter is to grant authorization to BerryDunn to conduct security testing and for the employees and/or agents of <client name> to work with BerryDunn in connection with the testing.

Due to the risk of performing such testing, the possibility of negative consequences, and to assure that it has adequate permission to conduct these tests, BerryDunn must obtain authorization to perform these scans and tests, and acceptance of that risk by <client name>.

By signing below, the undersigned (the "Authorizing Officer") confirms his/her authority to accept the risks described above and provide authorization to BerryDunn on behalf of <client name>, and that his/her signature will make this document binding upon <client name>.

Disclaimer and Limitation of Liability

In contracting BerryDunn to perform a Security Testing Assessment, including internal and/or external vulnerability scans, web application scans and penetration testing, <client name> acknowledges that the purpose of the scanning is to identify and report vulnerabilities in the <client name>'s computer network.

BerryDunn will take reasonable precautions to conduct the testing in a controlled manner and limit its activities to a safe level. The testing itself may affect the system(s) negatively in many ways. For example, it may decrease the performance levels of part or all of the system; cause availability of some or all services or data to be lost permanently or for an indeterminate period of time, possibly resulting in the need to reload data and systems from a backup or undertake a system rebuild; and/or cause problems which may require the system to be rebooted or result in attacks upon the system(s).

By signing below, the Authorizing Officer, on behalf of <client name>:

- a. Authorizes BerryDunn to perform the vulnerability scanning referenced in this document, as well as to undertake activities related to that scanning, and certifies that such scanning and related activities will not be considered to constitute: (i) trespass; (ii) unauthorized use of or access to <client name>'s computer systems or any <client name>'s software, or property; or (iii) a violation of law;
- b. Understands and accepts the risk that the scanning may have a negative effect on <client name>'s computer system(s) and agrees to indemnify BerryDunn, and BerryDunn's officers, directors, employees, contractors, agents, and attorneys (collectively, the "Indemnified Parties") and hold the Indemnified Parties harmless from liability arising from or related to any such negative effects unless caused by the gross



negligence or intentional malfeasance of BerryDunn or of any of the other Indemnified Parties when acting for BerryDunn; and

- c. Represents and warrants that <client name> has a complete and up to date data and system backup stored in a secure location that is isolated from and cannot be affected by the security testing.

<client name>

Signature

Name

Title

Department/Agency

Date

Appendix B: Requested Work Samples

On the following pages, we have included work samples representative of our executive summary reports and technical reports.

[REDACTED]

Security and Privacy Assessment Report

Deliverable version – V 2.0

Table of Contents

<u>Section</u>	<u>Page</u>
Table of Contents.....	i
1.0 Executive Summary.....	1
1.1 Risk Summary	1
1.1.1 Policy and Procedures Summary	1
1.1.2 Vulnerability Scanning and Penetration Testing Summary	1
1.1.3 Configuration Assessment and Administrative Risk Summary.....	2
1.2 Approach and Methodology	3
1.3 Relevant Standards	3
1.4 Acknowledgements.....	4
2.0 Scope.....	5
2.1 Components Tested.....	5
2.1.1 Web Applications.....	5
2.1.2 Linux Systems	5
2.1.3 Windows Server Systems.....	6
2.1.4 Database Systems	6
2.2 Documents Assessed	6
2.3 Personnel Interviewed	6
3.0 System Overview	8
3.1 Purpose of System.....	8
3.2 Goals and Objectives:.....	8
4.0 Security Analysis	10
4.1 Threats	10
4.2 Vulnerabilities	10
4.3 Likelihood	11
4.4 Impact.....	11
4.5 Risk Rankings.....	11

5.0	Summary of Findings.....	13
5.1	Assessment Results Summary	14
5.2	Configuration Assessment Results Summary	15
6.0	Recommendations	16
	Appendix A. Acronym List.....	17

Table i: Version History

Version	Date Delivered	Update Reason

1.0 Executive Summary

[REDACTED] has the responsibility to maintain, operate, and develop the [REDACTED]. Through the [REDACTED] BerryDunn was contracted to perform an independent security and privacy assessment of the [REDACTED]. The security and privacy assessment was performed from [REDACTED].

1.1 Risk Summary

1.1.1 Policy and Procedures Summary

BerryDunn has identified the following core opportunities for enhancing the [REDACTED] policies and procedures:

- ▲ The System Security Plan (SSP) lacks details related to the implementation, operation, and governance of the [REDACTED] system. The details of the recommended areas for improvement can be referenced within the Planning (PL) family PL-2 finding. Updating the SSP will take significant time and investment to accomplish, which may require a longer-term plan to address.
- ▲ Third party and supply chain management policies and procedures should be enhanced to align with Supply Chain Risk Management (SR) controls SR-1 and SR-2. The SR-1 and SR-2 controls should also be incorporated into [REDACTED]'s overall risk management strategy for managing the [REDACTED] environment.
- ▲ A number of National Institute of Standards and Technology (NIST) control family policies and procedures are rolled into related control family policies and procedures. An example of this is the Access Control and the Identification and Authentication policy and procedures. BerryDunn recommends that a separate set of policies and procedures are in place for each individual control family.
- ▲ From a policy governance perspective, BerryDunn recommends each policy should include language that defines the timing of the policy review cycle.

A complete analysis and supporting details may be found in the separate deliverable [REDACTED] Policy and Procedure Review Report.

1.1.2 Vulnerability Scanning and Penetration Testing Summary

BerryDunn has identified the following opportunities for enhancing the [REDACTED] security posture from the vulnerability scanning and penetration testing:

- ▲ Multiple Cross-Site (XSS) Scripting and Structured Query Language (SQL) Injection vulnerabilities were discovered in the web applications tested. Secure coding practices should be put in place to ensure that all data collected from the client is sanitized.
- ▲ Login Forms that submit in clear text were discovered. All login information should be encrypted.

- ▲ Insecure versions of Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols were detected in the environment, including SSLv3, TLS 1.0 and TLS 1.1. These insecure protocols should be disabled.
- ▲ TLS 1.2 is not enabled on all systems. This is the most secure protocol available and should be utilized on all systems.
- ▲ The public facing website [REDACTED] does not support Perfect Forward Secrecy (PFS) and allows clients to utilize weak cipher suites. PFS protects past sessions against future compromises of keys or passwords protects past sessions against future compromises of keys or passwords. Weak cipher suites should be disabled.

A complete analysis and supporting details may be found in the separate deliverable Vulnerability Scanning and Penetration Testing Report.

1.1.3 Configuration Assessment and Administrative Risk Summary

BerryDunn identified the following opportunities for enhancing the [REDACTED] security posture from the configuration reviews and the administrative review:

- ▲ Control implementations are not well defined within existing policy, plans and procedures. Generic descriptions about what is expected to be in place are commonplace.
- ▲ A configuration management plan is not in place. Procedures for maintaining configurations are not documented. Functionality, ports, protocols, software, and services that are unsuitable for use are not documented.
- ▲ System and service acquisition procedures do not include contractual language to ensure that the appropriate system documentation includes information about security and privacy control implementation.
- ▲ [REDACTED] relies on general risk management processes, rather than developing processes and procedures specific to acquiring systems, software, tools, and services.
- ▲ Security benchmarks are not consistently applied to all systems and technologies. Specific benchmarks should be applied to all Windows systems, Linux systems, and databases in use.

Table 1 below summarizes the number of risks by category that BerryDunn identified from the configuration and administrative risk review.

Table 1. Summary of Risks

Risk Category	Number of Risks
Critical	[REDACTED]
High	[REDACTED]
Moderate	[REDACTED]
Low	[REDACTED]

Risk Category	Number of Risks
Total Risks	[REDACTED]

1.2 Approach and Methodology

The approach and methodology of this assessment was split into several different parts. The first part was a review of [REDACTED]'s Information Technology Policies and Procedures to gain an understanding of [REDACTED]'s IT security and information security management and governance practices. Detailed analysis of this review is located in the [REDACTED] Policy and Procedure Assessment Report.

To develop this Policy and Procedure assessment report, BerryDunn reviewed and examined approximately forty-five policies, procedures, and standards. BerryDunn's review was performed against control requirements defined within the NIST SP 800-53 Rev. 5 moderate set of security and privacy controls. For each of the NIST SP 800-53 Rev. 5 control families, BerryDunn reviewed individual control requirements to identify gaps and developed recommendations that would allow for [REDACTED] policies and procedures to come into alignment with NIST framework.

The second part of the assessment was a configuration analysis of Linux systems, Windows systems, and databases. The scripts collect information that enables BerryDunn to evaluate the tests contained in the Safeguard Computer Security Evaluation Matrix (SCSEM), maintained by the Internal Revenue Service (IRS) Office of Safeguards, or based upon the Center for Internet Security (CIS) benchmarks. Because the IRS standards sometimes require more secure settings for controls, BerryDunn adjusted test criteria to better align with NIST 800-53 guidance. An artifact for each system type detailing all the tests performed is provided as part of the assessment.

The third and final part of the assessment was vulnerability scanning and penetration testing of the server infrastructure and the web applications. To complete this testing, BerryDunn used a series of commercially available tools and toolkits that included NMAP, Nessus, Metasploit, QualysGuard, and Kali Linux. Non-credential and credentialed application and vulnerability scans were performed to help identify potential vulnerabilities in the [REDACTED] external-facing (public) and internal-facing (private) footprints.

1.3 Relevant Standards

In order to evaluate that adequate security controls are in place, this assessment included an evaluation of policies, procedures, administrative controls, and system configurations to verify that minimum applicable security requirements are met as specified by the following standards:

- ▲ NIST Security and Privacy Controls for Information Systems and Organizations 800-53, Revision 5
- ▲ NIST Risk Management Framework 800-37, Revision 2
- ▲ NIST Guide for Conducting Risk Assessments 800-30, Revision 1

▲ NIST Cybersecurity Framework

1.4 Acknowledgements

The BerryDunn team would like to acknowledge and thank [REDACTED] leadership and staff for their cooperation and participation in all phases of this project. In addition, the BerryDunn team would like to especially thank [REDACTED] for their coordination, communications, and assistance throughout this project.

2.0 Scope

The [REDACTED] engaged BerryDunn to perform an onsite Security and Privacy Control Assessment (SCA) of the [REDACTED] in order to determine:

- ▲ If the system is compliant with NIST SP 800-53 Revision 5 moderate controls;
- ▲ If the underlying infrastructure supporting the system is secure;
- ▲ If the system and data are securely maintained; and
- ▲ If proper configuration associated with the database and file structure storing the data are in place.

The SCA consisted of configuration testing, documentation review, and vulnerability testing.

This Risk Analysis Report presents the results of a security and privacy assessment of the [REDACTED] and is provided to support the [REDACTED] program goals, efforts, and activities necessary to achieve compliance with the necessary security and privacy requirements.

2.1 Components Tested

BerryDunn conducted testing against the production and User Acceptance Testing (UAT) environment provided by [REDACTED].

The following components were tested during this assessment:

- ▲ [REDACTED]

2.1.1 Web Applications

Web application testing will consist of the Production and Test regions of the [REDACTED] applications. **Table 2** shows the uniform resource locator (URLs) that were identified for the scope of the testing.

Table 2 Web Applications Tested

Web Application	URL:
[REDACTED]	[REDACTED]

2.1.2 Linux Systems

Linux systems consisted of the Production region of [REDACTED]. **Table 3** identifies the systems in scope for testing.

Table 3 Linux Systems

IP Address or Range	Machine /Hostname	Operating System/Software and Version	Function
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

2.1.3 Windows Server Systems

Windows Server systems consisted of the Production and Test regions of [REDACTED]. **Table 4** identifies the windows systems in scope for testing.

Table 4 Windows Systems

IP Address or Range	Machine /Hostname	Operating System/Software and Version
[REDACTED]	[REDACTED]	[REDACTED]

2.1.4 Database Systems

Database systems consisted of the Production and Test regions of the [REDACTED] applications. **Table 5** shows the Systems that were identified for the scope of the testing

Table 5 Database Systems

IP Address or Range	Machine /Hostname	Database	Version
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

2.2 Documents Assessed

A complete list of policies, procedures, and documents that were reviewed may be found in the separate deliverable [REDACTED] Policy and Procedure Review Report.

2.3 Personnel Interviewed

The assessor interviewed business, information technology, and support personnel to help ensure effective implementation of operational and managerial security and privacy controls across all support areas. Interviews were customized to focus on control assessment procedures that apply to individual roles and responsibilities and assure proper implementation and/or execution of security and privacy controls.

Table 6 identifies the personnel selected to be interviewed had the following roles:

Table 6 Personnel Interviewed

Title	Name of Person	Date of Interview	Organization
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

Title	Name of Person	Date of Interview	Organization
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

3.0 System Overview

The [REDACTED] [REDACTED] is an internet-facing, multi-tier web application which started development in the 1990s. The business processes and technology that support [REDACTED] are located in the [REDACTED] area. The primary datacenter is located in [REDACTED] and the failover datacenter is located in [REDACTED]. The application is accessible to end users via a web browser. The [REDACTED] of [REDACTED] uses the [REDACTED] system for Title XIX program control and administrative costs; service to recipients, providers, and inquiries; operations of claims control and computer capabilities; and management reporting for planning and control.

3.1 Purpose of System

The primary application assists staff with the claims and encounter processing, provider payment, and reporting business functions including recording, sorting, and classifying claims; issuing checks or notices of denial of claims; issuing monthly invoices for spenddown and premium collections; and reporting. Web portals facilitate system interactions for staff and providers. Providers submit either electronic Health Insurance Portability and Accountability Act of 1996 (HIPAA) compliant Electronic Data Interchange transactions or direct data entry via portal or paper. Most all claims (99%) are submitted electronically. Paper claims are scanned or manually entered into the [REDACTED]. Once claims are in the [REDACTED], various batch processes and jobs are used to complete the claims adjudication, payment, and other processes. The current [REDACTED] processes over millions of claims received from over 800 claims transactions submitters representing an average of over 8,000 providers in each payment cycle yearly.

3.2 Goals and Objectives:

Identification and assessment of security risks related to the development and operation of the [REDACTED] including areas of concern based on the risk to the continuity of [REDACTED] functions and to the confidentiality, privacy, integrity, and availability of critical, personally identifiable data in the context of best practices and the requirements of the HIPAA and other [REDACTED] and federal privacy and security laws. Objectives shall include:

- ▲ Review of existing [REDACTED] and [REDACTED] security and information management policies, practices, procedures, technologies, and business associate requirements currently in place
- ▲ Identification and assessment of the value of critical assets, applications, staff, infrastructure, and processes
- ▲ Identification of internal and external threats and weaknesses to the critical assets and processes;
- ▲ Identification of known risks inherent to the computing infrastructure, development tools, and application systems (commercial off-the-shelf and custom-developed applications)

- ▲ Identification of risks related to the continuity of solution's functions including misuse of data, loss of data, and application error
- ▲ Assignment of quantitative and/or qualitative values to each threat based on the identified weaknesses and value of the critical assets
- ▲ Collaboration with [REDACTED] and Information[REDACTED] to qualify and quantify the probability of realization and business impact of the identified risks and prioritize the risks accordingly.

Development of a realistic action plan in the context of the environment and available resources to mitigate the identified risks. Objectives shall include:

- ▲ Identify areas demonstrating high risk that should have the immediate attention of [REDACTED] and [REDACTED] resources for risk mitigation
- ▲ Provide recommendations to mitigate or remediate each identified risk of solution(s) listed in the [REDACTED]
- ▲ Propose a methodology for use by [REDACTED] and the solution vendor for analyzing, prioritizing, and mitigating identified risks and documenting risk mitigation activities.
- ▲ Identification of activities that can be conducted by [REDACTED] Privacy and Security staff to monitor and improve [REDACTED] and the solution vendor's Privacy and Security functions and outcomes related to [REDACTED].

4.0 Security Analysis

BerryDunn followed the guidance provided by NIST SP 800-30, Revision 1: *Guide for Conducting Risk Assessments* to assess the risk to [REDACTED]'s information system. Non-compliant and partially compliant controls were then evaluated for the likelihood that a weakness in a control would be exploited by a threat, and the impact that would have on the [REDACTED]'s information system and business operations. The objective of this evaluation is to assess, qualitatively, the risk exposure to the [REDACTED] if a weakness remains uncorrected.

Our risk assessment is a qualitative one, meaning that the assignment of likelihood and impacts to risk is subjective. Therefore, it is important to note that the risk scores contained in this report serve as a baseline. There may be other mitigating factors that were not captured in the discovery process that would lower, or elevate, risks.

4.1 Threats

A threat can be defined as an event with the ability to exploit a vulnerability. There are several types of threat sources that have the potential to impact a system negatively. These are listed in **Table 7** below.

Table 7 Threat Source Types¹

Threat Source Types	Description
Adversarial	Individuals, groups, organizations, or [REDACTED] s that seek to exploit the organization's dependence on cyber resources (i.e., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies).
Accidental	Erroneous actions taken by individuals in the course of executing their everyday responsibilities.
Structural	Failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances, which exceed expected operating parameters.
Environmental	Natural disasters and failures of critical infrastructures on which the organization depends, but which are outside the control of the organization.

4.2 Vulnerabilities

A vulnerability is a weakness that has the potential to be exploited by a threat source. Often, these weaknesses are derived from security controls that are not in place or only partially implemented. New threats continually arise over time, which may exploit a previously undiscovered weakness. In addition, there is a potential for security controls to degrade in

¹ National Institute of Standards and Technology Special Publication 800-30 Rev.1, Appendix D, page D-2

effectiveness over time. Therefore, it is critical to provide continual protection to the system by following best practices for Governance, Risk management, and Compliance (GRC).

4.3 Likelihood

The likelihood of harm to occur from a threat event is based on the vulnerability's potential for exploitation, historical data, and empirical evidence—or, in the case of an adversarial threat, the intent, capability, and targeting by the adversary. Often, it will be assessed with respect to time. It should be noted that this does not necessarily measure the likelihood of an event occurring, but the likelihood of harm to occur from the impact of a successful threat event. Likelihood is ranked as the following:

1. Not Likely (~10%)
2. Low Likelihood (~30%)
3. Likely (~50%)
4. Highly Likely (~70%)
5. Near Certainty (~90%)

4.4 Impact

The impact that a threat can have is the degree of damage to an organization or its systems that could result should a threat event occur. Impacts were calculated using a simple 1-5 methodology:

1. Minimal – Little or no impact to the information system
2. Minor – Disruption to the information system that is easily corrected
3. moderate – Deliberate disruption to the information system that requires resources and time to correct
4. Significant – Serious disruption to the information system that may deteriorate or halt the ability of the organization to provide services that require appreciable resources to remediate
5. Severe – Complete disruption of the information system that halts the organization's ability to perform or provide services; includes the loss of critical data and system assets

4.5 Risk Rankings

The risk rankings in this report express a qualitative assessment of how effective the safeguards put in place by the [REDACTED] are meeting the moderate control objectives as prescribed by NIST. Risk is calculated by determining the likelihood and the impact caused if the identified vulnerability is exploited. As noted in the previous section, qualitative risk ratings are subjective and rely on the experience and expertise of the assessor to ensure that the right risk rating is applied to the control. The assessor may look at different threat types (ransomware, insider threat, etc.) and apply knowledge of how a particular vulnerability is exploited by a particular threat actor.

Figure 1 below defines how risk ratings are derived from impact and likelihood.

Figure 1 Risk Rating

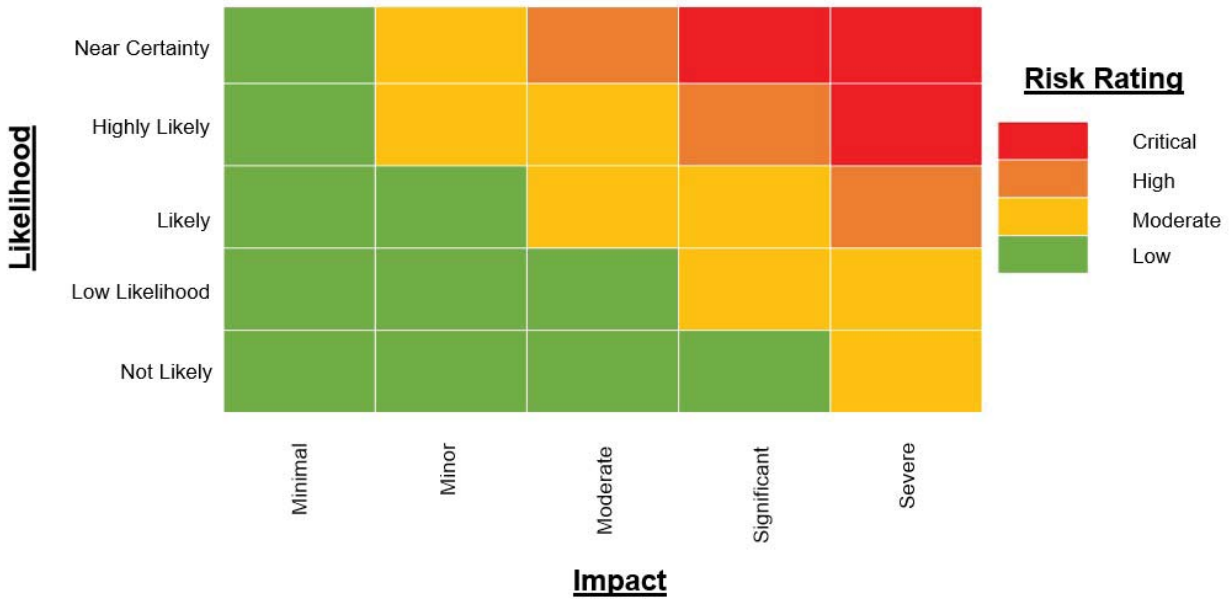


Table 8 below provides definitions for each risk level. These levels represent the degree or level of risk to which an IT system, facility, or procedure might be exposed, based on the above factors.

Table 8 Risk Definitions

Risk Rank	Definition
Critical	Corrective actions to system should be taken immediately by Authorizing Official.
High	There is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan should be put in place as soon as possible.
Moderate	Corrective actions are needed, and a plan should be developed to incorporate these actions within a reasonable period of time.
Low	The system's Authorizing Official should determine whether corrective actions are still required.

5.0 Summary of Findings

BerryDunn's personnel interviews and documentation review found that controls were not well documented within policy, plans, and procedures. When documentation defines controls in place, it was common to find generic comments about what is expected to be in place rather than defining the actual control in use. System documentation should be reviewed and revised annually, or when significant changes to the system are implemented.

The policy and procedure review found that there is no configuration management plan in place. Baseline configurations do not have a defined process that is being followed for maintenance and updates. Unnecessary functionalities, ports, protocols, software, and services have not been documented, making it difficult to complete a thorough review for configurations that should not be in place on systems. Without detailed plans, policies and procedures configurations will drift from standards over time and security risks will increase with time.

System and service acquisition procedures do not ensure that contractual language is included requiring that security and privacy controls are appropriately implemented and documented in system documentation. Without contractual language, security controls documentation may not be documented properly.

[REDACTED] does not have any documented procedures for supply chain risk management specific to acquiring systems or tools. [REDACTED] relies on their general risk management processes to assist with supply chain issues, potentially allowing risks related to acquired systems or services that may not be automatically considered, such as the insertion or use of counterfeits, tampering, theft, insertion of malicious software and hardware, and poor manufacturing and development practices in the supply chain.

[REDACTED] is still in the process of implementing tools to support their processes. These include tools like ManageEngine, which will improve system patching throughout the [REDACTED] environment, and Qualys File Integrity monitoring (FIM) which will monitor and detect changes in files that may indicate a cyberattack. Fully implementing these tools will improve the security posture of the [REDACTED] system.

There is no automated process in place to support most of the processes that [REDACTED] is using. Considering the use of automated processes within the environment can help mature processes to a better level of efficiency. NIST specifically suggests automated processes to support account management activities, incident response activities, and configuration management controls.

The configuration assessment revealed that there were inconsistencies in relation to applying benchmarks throughout the systems. Based on interviews with [REDACTED], it was identified that CIS benchmarks are expected to be applied and then systems should be adjusted based upon the specific function. During our review of current configurations, we noted some of the following areas as having a noticeable difference from benchmarking:

▲ [REDACTED]

5.1 Assessment Results Summary

Table 9 below indicates the assessment results by control assessment category based on this assessment. Detailed analysis and findings are in the documented in the Security Assessment Workbook (SAW) artifact.

Table 9 Summary of Assessment Results

Control Assessment Category	Count
Met	[REDACTED]
Partially Met	[REDACTED]
Not Met	[REDACTED]
TOTAL	[REDACTED]

Table 10 below shows the assessment results based on control families.

Table 9 Summary of Assessment Results by NIST Control Family

Security and Privacy Control Family	Met	Partially Met	Not Met	Total
AC – Access Control	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
AT – Awareness and Training	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
AU – Audit and Accountability	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
CA - Assessment, Authorization, and Monitoring	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
CM – Configuration Management	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
CP – Contingency Planning	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
IA – Identification and Authentication	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
IR – Incident Response	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
MA – Maintenance	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
MP – Media Protection	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
PE – Physical and Environmental Protection	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
PL – Planning	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
PM – Program Management	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
PS – Personnel Security	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

Security and Privacy Control Family	Met	Partially Met	Not Met	Total
	D]			
PT - Personally Identifiable Information Processing and Transparency	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
RA – Risk Assessment	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
SA – System and Services Acquisition	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
SC – System and Communications Protection	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
SI – System and Information Integrity	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
SR - Supply Chain Risk Management	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
TOTAL	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

5.2 Configuration Assessment Results Summary

For the purposes of this report, BerryDunn is reporting the server and database configuration assessment items that are rated as Critical, High, and Moderate risks. Detailed analysis and findings for all risks, including the low-risk findings, are documented in the SAW artifact. **Table 11** shows the configuration assessment results based on risk level.

Table 10 Summary of Configuration Assessment Results

Risk Level	Infrastructure Scripts	Database Scripts	Total
Critical	[REDACTED]	[REDACTED]	[REDACTED]
High	[REDACTED]	[REDACTED]	[REDACTED]
Moderate	[REDACTED]	[REDACTED]	[REDACTED]
TOTAL	[REDACTED]	[REDACTED]	[REDACTED]

6.0 Recommendations

For each finding, the assessor developed detailed recommendations for improvements that address the findings and the business and system risks. Most of the recommendations in this document fall into the following areas:

- ▲ Review and update plans, policies, and procedures to include appropriately detailed control descriptions that are in place for the system instead of general control expectations for what should be in place.
- ▲ Develop a configuration management plan and processes that follow the requirements included in the Configuration Management family of NIST SP 800-53 Rev. 5 moderate controls. Some of the specific processes that should be developed include documented processes related to handling baseline configurations, including how baselines are maintained for each type of system used in the [REDACTED] environment, where they are stored, and how to roll back when necessary.
- ▲ Improve system and service acquisition processes and documentation to ensure system documentation related to privacy and security implementations are provided as part of requirements.
- ▲ Complete the implementation and configuration of [REDACTED] to improve [REDACTED]'s security posture and ensure that effective system and information integrity controls are in place.
- ▲ Complete a review of configurations currently in place across all affected systems and ensure that benchmarks are being appropriately utilized for configuring and protecting systems and data on those systems.
- ▲ Consider the implementation of automated tools to aid in processes related to account management processes, incident response activities, and configuration management.

Appendix A. Acronym List

Table 11 Acronym List

Acronym	Definition
AC	Access Control
AT	Awareness and Training
AU	Audit and Accountability
CA	Assessment, Authorization, and Monitoring
CIS	Center for Internet Security
CM	Configuration Management
CP	Contingency Planning
FIM	File Integrity Monitoring
GRC	Governance, Risk Management, and Compliance
HIPAA	Health Insurance Portability and Accountability Act of 1996
IA	Identification and Authentication
IR	Incident Response
IRS	Internal Revenue Service
ITSD	Information Technology Services Division
MA	Maintenance
MP	Media Protection
NIST	National Institute of Standards and Technology
PE	Physical and Environmental Protection
PFS	Perfect Forward Secrecy
PL	Planning
PM	Program Management
PS	Personnel Security
RA	Risk Assessment
SA	System and Services Acquisition
SAW	Security Assessment Workbook
SC	System and Communications Protection
SCA	Security and Privacy Control Assessment
SCSEM	Safeguard Computer Security Evaluation Matrix
SI	System and Information Integrity
SQL	Structured Query language
SR	Supply Chain Risk Management
SSL	Secure Socket Layer

Acronym	Definition
SSP	System Security and Privacy Plan
TLS	Transport Layer Security
UAT	User Acceptance Testing
URL	Uniform Resource Locator
XSS	Cross-Site Scripting

<Redacted>'s

Vulnerability Scanning and Penetration Testing Report

Version 0.1 (Draft)

Submitted by:

BerryDunn
2211 Congress Street
Portland, ME 04102-1955
207.541.2200

Bill Brown, Principal

bbrown@berrydunn.com

Matthew Bria, Project Manager

mbria@berrydunn.com

Submitted On:

26 October 2021

Table of Contents

<u>Section</u>	<u>Page</u>
Table of Contents.....	i
1.0 Executive Summary.....	1
1.1 Vulnerability Scanning and Penetration Testing Summary.....	1
1.2 Approach and Methodology	4
1.3 Scope	4
1.4 Relevant Standards	7
1.5 Acknowledgements.....	8
2.0 Technical Assessment	9
2.1 Assessment Overview	9
2.2 Transport Layer Security (TLS) and Secure Sockets Layer (SSL) Testing.....	9
2.3 Penetration and Exploitation Testing	18
2.3.1 Open Port Map.....	19
2.3.2 Default Web Pages	20
2.3.3 Server Message Block (SMB) Exploits	21
2.3.4 WebSphere Exploits.....	21
2.3.6 SNMP Exploits	22
2.3.7 Cross-Site Scripting (XSS).....	22
2.3.8 Blind SQL Injection.....	23
2.3.9 Insecure Login Forms.....	24
2.4 .NET Framework Information.....	24

Table i: Version History

Version	Date Delivered	Update Reason
Draft	26 October 2021	Initial Draft

1.0 Executive Summary

The < REDACTED>'s is an internet-facing, multi-tier web application. The business processes and technology that support <REDACTED> are located in the <Redacted>, <Redacted> area. The primary datacenter is located in <Redacted> and the failover datacenter is located in <Redacted>. The application is accessible to end users via a web browser. The <Redacted> uses the <REDACTED> system for Title XIX program control and administrative costs; service to recipients, providers, and inquiries; operations of claims control and computer capabilities; and management reporting for planning and control.

BerryDunn was contracted to perform vulnerability scanning and penetration testing against the <REDACTED> environment. The scope and systems that were tested are defined in detail within this report.

Over the course of the vulnerability scanning and penetration testing, BerryDunn did identify a number of High priority issues. **Please Note:** All changes should be thoroughly tested in lower environments before deploying into production to ensure that services are not negatively impacted by any change. **Table 1** summarizes the issues that BerryDunn has identified.

Table 1: High Priority Issues

Category	Issue	Priority	Reference
TLS Best Practices	<Redacted> does not support forward secrecy	High	https://blog.qualys.com/product-tech/2013/06/25/ssl-labs-deploying-forward-secrecy
TLS Best Practices	<Redacted> utilizes weak Cipher suites	High	https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices
Vulnerable Software	Older versions of the DotNet Framework are installed	High	https://support.microsoft.com/en-us/topic/resolving-view-state-message-authentication-code-mac-errors-6c0e9fd3-f8a8-c953-8fbe-ce840446a9f3
Web Application Coding Practices	XSS vulnerabilities where discovered	High	https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html
Web Application Coding Practices	Blind SQL Injection	High	https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

1.1 Vulnerability Scanning and Penetration Testing Summary

BerryDunn identified four issues with the Secure Sockets Layer (SSL) implementations on websites in scope. **Table 2** summarizes these findings. Detailed test results are located in section 2.2 of this report.

Table 2: Secure Sockets Layer (SSL) Vulnerability Summary

Issue
Forward Secrecy: Weak Key Exchange
Insecure Protocol in Use (SSL v3.0)
Insecure Protocol in Use (TLS v1.0)
Insecure Protocol in Use (TLS v1.1)
SHA1 certificates in use
Poodle Vulnerability
Weak Ciphers Available

Penetration testing was conducted against external facing components of the <REDACTED> environment. **Table 3** summarized the tests conducted. Detailed test results are located in section 2.3 of this report.

Table 3: Penetration Test Summary

Exploitation Description	Status
SMB Enumerate Users	Successfully identified local user accounts
SMBv1 EternalBlue Vulnerability	SMBv1 was detected on <Redacted>and <Redacted> Both systems were not vulnerable to the attack.
WebSphere Java Deserialization Vulnerability [<Redacted>	Session was not successfully created.
WebSphere Snoop Servlet Information Disclosure	Successful, information about the system was disclosed.
Tomcat CGI Servlet enableCmdLineArguments Vulnerability	Unsuccessful
SNMP Enumeration	Information about the environment was successfully disclosed.
Cross-Site (XSS) Scripting Vulnerabilities	Multiple vulnerabilities were confirmed.
Blind SQL Injection Vulnerability	One instance was detected.
Login form submitted in clear text	Two instances detected.

Web application testing was conducted on web sites in environment. **Table 4** summarizes the vulnerabilities that were confirmed during testing. Detailed test results are located in section 2.5 of this report.

Table 4: Confirmed Web Application Vulnerability Summary

Web Application	Urgent	Critical	Serious	Medium	Minimal	Total
<Redacted>	<Redacted>	2	66	0	0	78

<Redacted>	2	4	12	1	0	19
<Redacted>	11	2	15	0	1	29
<Redacted>	2	2	6	0	2	12
<Redacted>	0	8	4	0	0	12
<Redacted>	0	4	3	0	0	7
<Redacted>	4	2	13	1	0	20
<Redacted>	6	1	3	0	3	13
<Redacted>	4	1	11	0	9	25
<Redacted>	3	47	4	0	8	62
<Redacted>	<Redacted>	38	67	0	0	115
<Redacted>	0	19	8	0	0	27
Total	23	2	212	130	52	419

Table 5 summarizes the potential web application vulnerabilities that may exist, but were not able to be verified.

Table 5: Potential Web Application Vulnerability Summary

Web Application	Urgent	Critical	Serious	Medium	Minimal	Total
<Redacted>	0	0	1	0	1	2
<Redacted>	0	0	0	0	1	1
<Redacted>	0	0	1	0	0	1
<Redacted>	0	0	0	0	1	1
<Redacted>	0	0	0	0	9	9
<Redacted>	0	0	0	0	9	9
Total	0	0	2	0	21	23

Table 6 summarizes the number of vulnerabilities discovered during internal testing of the infrastructure and databases. The following observations are noted:

- Application software including <Redacted>
- The majority of the vulnerabilities identified are associated with <Redacted> patches vulnerabilities without updating the package version number, a practice known as backporting. This practice can result in false positives during vulnerability scans. <REDACTED> and <Redacted> should ensure software updates and patches are applied in a timely manner that aligns with documented enterprise standards.
- Insecure SSL 3.0, TLS v1.0 and TLS v1.1 is in use, along with weak and insecure cipher suites. TLS v1.2 should be used, SSL v3.0 and TLS v1.0 should be disabled. Strong cipher suites should be preferred.

Detailed test results are located in section 2.6 of this report.

Table 6: Infrastructure and Database Vulnerabilities Summary

Category	Critical	High	Medium	Low	Total
<Redacted>	3	55	91	12	161
<Redacted>	3	7	6	0	16
<Redacted>	0	4	5	1	<Redacted>
<Redacted>	0	0	4	2	6
<Redacted>	0	3	6	1	<Redacted>
<Redacted>	0	0	3	0	3
<Redacted>	1	2	3	4	<Redacted>
Total	7	71	118	20	216

1.2 Approach and Methodology

To meet the objectives of the assessment, BerryDunn developed the Rules of Engagement (RoE) that defined the approach and methodology, and the scope. Throughout the course of the audit, weekly checkpoint meetings were conducted between BerryDunn and <REDACTED> staff.

The technical review consisted of external-facing (public) and internal web application scanning; internal vulnerability scanning; and penetration testing.

Web Application, Vulnerability Scanning, and Penetration Testing: BerryDunn performed a reconnaissance scan of the external-facing (public) network components, and in doing so, identified potential targets that would be included in the scope of the testing. The RoE defined the approach and targets that would be included in the testing. Prior to commencing testing, the RoE were agreed upon and signed by the <REDACTED> representatives and the BerryDunn project principal.

To complete the testing, BerryDunn used a series of commercially available tools and toolkits that included NMAP, Nessus, MetaSploit, QualysGuard, and Kali Linux. Non-credential and credentialed application and vulnerability scans were performed to help identify potential vulnerabilities in the <REDACTED> external-facing (public) footprint.

1.3 Scope

The scope of BerryDunn’s vulnerability testing was the <REDACTED> Production, Test, and Development systems. These systems are described in **Table 7** below.

Table 7: Vulnerability Assessment Targets

IP Address or Range	Machine /Hostname	Operating System/Software and Version	Function
<Redacted>	<Redacted>	<Redacted>	<Redacted>

IP Address or Range	Machine /Hostname	Operating System/Software and Version	Function
<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>

For the external-facing (public) technical review BerryDunn tested Production systems. **Table 8** provides the internet protocol (IP) addresses and uniform resource locator (URLs) that were identified for the scope of the testing.

Table 8: External-Facing (Public) Targets

IP Address	DNS Record
<Redacted>	<Redacted>
<Redacted>	<Redacted>
<Redacted>	<Redacted>
<Redacted>	<Redacted>

Web application testing will consist of the Production and Test regions of the <REDACTED> applications. **Table 9** shows the uniform resource locator (URLs) that were identified for the scope of the testing.

Table 9: Web Application Targets

Web Application	URL:
<Redacted>	<Redacted>
<Redacted>	<Redacted>
<Redacted>	<Redacted>

Web Application	URL:
<Redacted>	<Redacted>
<Redacted>	<Redacted>
<Redacted>	<Redacted>
<Redacted>	<Redacted>
<Redacted>	<Redacted>
<Redacted>	<Redacted>
<Redacted>	<Redacted>
<Redacted>	<Redacted>
<Redacted>	<Redacted>
<Redacted>	<Redacted>
<Redacted>	<Redacted>

The following roles were used for web application testing:

Table 10: Web Application Roles

Web Application	Login ID
<Redacted>	<Redacted>
<Redacted>	<Redacted>
<Redacted>	<Redacted>
<Redacted>	<Redacted>
<Redacted>	<Redacted>
<Redacted>	<Redacted>
<Redacted>	<Redacted>
<Redacted>	<Redacted>
<Redacted>	<Redacted>

1.4 Relevant Standards

To evaluate that <REDACTED> and <Redacted> has adequate security controls in place, the separate assessment included a review and evaluation of the <REDACTED> policies and

procedures to verify that they meet the minimum applicable security requirements as specified by the following standards:

- National Institute of Standards and Tehnology (NIST) 800-53, Revision 5
- NIST Cybersecurity Framework

1.5 Acknowledgements

<Redacted>

2.0 Technical Assessment

2.1 Assessment Overview

The following sections contain the results of the vulnerability scanning and penetration testing of external-facing (public) components of the <REDACTED> environment. Vulnerability scanning and penetration testing activities took place from <REDACTED>. Testing activities took place between 12:00AM and 6:00AM Central Daylight Time (CDT). Prior to commencing testing and at the conclusion of testing each day, BerryDunn notified the identified <REDACTED> and <Redacted> contacts via email on testing status. A variety of commercially available tools, including QualysGuard, Nessus, and Kali Linux, were used to conduct testing.

Table 7, 8 and 9 in section 1.3 identify the IP addresses and URLs defined as being in scope for the testing activities.

2.2 Transport Layer Security (TLS) and Secure Sockets Layer (SSL) Testing

The following are the TLS issues that were observed in the <REDACTED> environment:

Table 11: TLS Issues

Issue	Priority	Rationale	Reference
<Redacted> does not support forward secrecy	High	External facing systems are high risk	https://blog.qualys.com/product-tech/2013/06/25/ssl-labs-deploying-forward-secrecy
<Redacted> utilizes weak Cipher suites	High	External facing systems are high risk. This is closely related to the Forward Secrecy issue above	https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices
TLS 1.2 is not enabled on all systems	Moderate	Secure functionality is not available for use	https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices
Insecure versions of SSL and TLS were detected in the environment	Moderate	Only internal communications is affected.	https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices
Obsolete SHA 1 certificates are in use on internal systems: <Redacted>	Low	Certificates are in use, and internal only.	https://blog.qualys.com/product-tech/2014/09/09/sha1-deprecation-what-you-need-to-know

BerryDunn used QualysGuard to perform a series of SSL checks on the in-scope external-facing (public) URLs. The purpose of these checks was to identify any insecure protocols or services that may be susceptible to an attack and to assess the external footprint of the <REDACTED> application. **Table 12** provides an overview of the supported protocols and vulnerabilities that were identified for the in-scope web applications.

Table 12: External (Public) Supported Protocols

Certificate Expires	Forward Secrecy	RC4 Supported	TLS	TLS	TLS	TLS 1.0	SSL 3.0	SSL 2.0
			1.3	1.2	1.1		Insecure	Insecure
<Redacted>								
<Redacted>	ROBUST	No	No	Yes	No	No	No	No
<Redacted>								
<Redacted>	ROBUST	No	Yes	Yes	No	No	No	No
<Redacted>								
<Redacted>	ROBUST	No	No	Yes	No	No	No	No
<Redacted>								
<Redacted>	ROBUST	No	No	Yes	No	No	No	No

A series of tests were performed to check and verify for potential SSL vulnerabilities of the in-scope external-facing (public) URLs. **Table 13** summarizes the results of the tests.

Table 13: External-Facing (Public) SSL Vulnerability Tests

Heart-beat	Beast	Drown	Heart-bleed	OpenSSL Ccs	OpenSSL Lucky Minus 20	Poodle	Poodle TLS
<Redacted>							
No	No	No	No	No	No	Not Vulnerable	Not Vulnerable
<Redacted>							
No	No	No	No	No	No	Not Vulnerable	Not Vulnerable
<Redacted>							
No	No	No	No	No	No	Not Vulnerable	Not Vulnerable
No	No	No	No	No	No	Not Vulnerable	Not Vulnerable

BerryDunn used a custom script to perform a series of SSL checks on the in-scope internal-facing URLs. The purpose of these checks was to identify any insecure protocols or services that may be susceptible to an attack and to assess the external footprint of the <REDACTED> application. **Table 14** provides an overview of the supported protocols and vulnerabilities that were identified for the in-scope web applications.

Table 14: Internal Supported Protocols

Certificate	Forward Secrecy	RC4 Supported	TLS	TLS	TLS	TLS	SSL 3.0	SSL 2.0
			1.3	1.2	1.1	1.0	Insecure	Insecure
<Redacted>								
sha256WithRSA Encryption (part of chain is SHA-1 With RSA Encryption)	Robust	No	No	Yes	No	No	No	No
<Redacted>								
SHA-1 With RSA Encryption	Weak	Yes	No	Yes	Yes	Yes	Yes	No
<Redacted>								
SHA-1 With RSA Encryption	Weak	Yes	No	Yes	Yes	Yes	Yes	No
<Redacted>								
SHA-1 With RSA Encryption	Weak	No	No	Yes	Yes	Yes	No	No

A series of tests were performed to check and verify for potential SSL vulnerabilities of the in-scope Internal-facing URLs. **Table 15** summarizes the results of the tests.

Table 15: Internal-Facing SSL Vulnerability Tests

Heart-beat	Beast	Drown	Heart-bleed	OpenSSL Ccs	OpenSSL Lucky Minus 20	Poodle	Poodle TLS
<Redacted>							
No	No	No	No	No	No	No	Not Vulnerable
<Redacted>							
No	Yes	No	No	No	No	Yes	Not Vulnerable

Heart-beat	Beast	Drown	Heart-bleed	OpenSSL Ccs	OpenSSL Lucky Minus 20	Poodle	Poodle TLS
<Redacted>							
No	Yes	No	No	No	No	Yes	Not Vulnerable
<Redacted>							
No	Yes	No	No	No	No	No	Not Vulnerable

Next we tested to verify if there were any weak encryption ciphers present on the identified in-scope URLs. **Table 16, 17, 18, 19, 20, 21, and 22** provide a list of identified weak ciphers. <REDACTED> staff should review the weak ciphers that are in use and upgrade to stronger ciphers where possible.

Table 16: Weak Cipher Identification: <Redacted>

Ciphers	www.<Redacted>med.com
TLS_RSA_WITH_AES_128_CBC_SHA	WEAK
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	WEAK
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	WEAK
TLS_RSA_WITH_AES_128_CBC_SHA256	WEAK
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	WEAK
TLS_RSA_WITH_AES_128_GCM_SHA256	WEAK
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	SECURE
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	WEAK
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	SECURE
TLS_RSA_WITH_AES_256_CBC_SHA	WEAK
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	WEAK
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	WEAK
TLS_RSA_WITH_AES_256_CBC_SHA256	WEAK
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	WEAK
TLS_RSA_WITH_AES_256_GCM_SHA384	WEAK
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	SECURE
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	SECURE

Table 17: Weak Cipher Identification: <Redacted>

Ciphers	<Redacted>	<Redacted>
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	SECURE	SECURE
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	SECURE	SECURE
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	WEAK	WEAK
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA2	WEAK	WEAK
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	WEAK	WEAK
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	WEAK	WEAK
TLS_RSA_WITH_AES_256_GCM_SHA384	WEAK	WEAK
TLS_RSA_WITH_AES_128_GCM_SHA256	WEAK	WEAK
TLS_RSA_WITH_AES_256_CBC_SHA256	WEAK	WEAK
TLS_RSA_WITH_AES_128_CBC_SHA256	WEAK	WEAK
TLS_RSA_WITH_AES_256_CBC_SHA	WEAK	WEAK
TLS_RSA_WITH_AES_128_CBC_SHA	WEAK	WEAK

Table 18: Weak Cipher Identification: <Redacted>

Ciphers	<Redacted>
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	SECURE
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	SECURE
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	WEAK
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	WEAK
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	WEAK
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	WEAK
TLS_RSA_WITH_AES_256_GCM_SHA384	WEAK
TLS_RSA_WITH_AES_128_GCM_SHA256	WEAK
TLS_RSA_WITH_AES_256_CBC_SHA256	WEAK
TLS_RSA_WITH_AES_128_CBC_SHA256	WEAK
TLS_RSA_WITH_AES_256_CBC_SHA	WEAK

Ciphers	<Redacted>
TLS_RSA_WITH_AES_128_CBC_SHA	WEAK

Table 19: Weak Cipher Identification: <Redacted>

Ciphers	<Redacted>
AES128-GCM-SHA256	STRONG
AES256-GCM-SHA384	WEAK
AES128-SHA256	WEAK
AES256-SHA256	WEAK
AES128-SHA	WEAK
AES256-SHA	WEAK
DES-CBC3-SHA	WEAK
ECDHE-RSA-AES128-SHA256	WEAK
ECDHE-RSA-AES256-SHA384	WEAK
ECDHE-RSA-AES128-GCM-SHA256	WEAK
ECDHE-RSA-AES256-GCM-SHA384	STRONG
NULL-SHA256	INSECURE
NULL-SHA	INSECURE
ECDHE-RSA-NULL-SHA	INSECURE
RC4-SHA (TLS_RSA_WITH_RC4_128_SHA)	INSECURE
RC4-MD5 (TLS_RSA_WITH_RC4_128_MD5)	INSECURE
DES-CBC-SHA	WEAK
NULL-MD5	INSECURE
EXP-RC4-MD5 (TLS_RSA_EXPORT_WITH_RC4_40_MD5)	INSECURE
EXP-RC2-CBC-MD5 (TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5)	INSECURE

Table 20: Weak Cipher Identification: e<REDACTED>.<Redacted>med.com

Ciphers	e<REDACTED>.<Redacted>med.com
ECDHE-RSA-AES256-GCM-SHA384	STRONG
ECDHE-RSA-AES128-GCM-SHA256	STRONG
ECDHE-RSA-AES256-SHA384	WEAK
ECDHE-RSA-AES128-SHA256	WEAK
ECDHE-RSA-AES256-SHA	WEAK
ECDHE-RSA-AES128-SHA	WEAK
ECDHE-RSA-DES-CBC3-SHA	WEAK
AES256-GCM-SHA384	STRONG
AES128-GCM-SHA256	STRONG
AES256-SHA256	WEAK
AES128-SHA256	WEAK
AES256-SHA	WEAK
AES128-SHA	WEAK
DES-CBC3-SHA	WEAK

Table 21: Weak Cipher Identification: myworkspace.<Redacted>med.com

Ciphers	myworkspace.<Redacted>med.com
ECDHE-RSA-AES256-GCM-SHA384	STRONG
DHE-RSA-AES256-GCM-SHA384	STRONG
ECDHE-RSA-AES128-GCM-SHA256	STRONG
DHE-RSA-AES128-GCM-SHA256	SECURE
ECDHE-RSA-AES256-SHA384	WEAK
DHE-RSA-AES256-SHA256	WEAK
ECDHE-RSA-AES256-SHA	WEAK
DHE-RSA-AES256-SHA	WEAK
ECDHE-RSA-AES128-SHA256	WEAK
DHE-RSA-AES128-SHA256	WEAK
ECDHE-RSA-AES128-SHA	WEAK

Ciphers	myworkspace.<Redacted>med.com
AES256-GCM-SHA384	STRONG
AES256-SHA256	WEAK
AES256-SHA	WEAK
AES128-SHA256	WEAK
AES128-SHA	WEAK
DES-CBC3-SHA	WEAK

Table 22: Weak Cipher Identification: filenet.<Redacted>med.com

Ciphers	<Redacted>
AES128-SHA	WEAK
AES256-SHA	WEAK
AES128-GCM-SHA256	STRONG
AES256-GCM-SHA384	STRONG
ECDHE-RSA-AES128-SHA	WEAK
ECDHE-RSA-AES256-SHA	WEAK
ECDHE-RSA-AES128-SHA256	WEAK
ECDHE-RSA-AES256-SHA384	WEAK
ECDHE-RSA-AES128-GCM-SHA256	STRONG
ECDHE-RSA-AES256-GCM-SHA384	STRONG
AES128-SHA256	WEAK
AES256-SHA256	WEAK
TLS13-AES-128-GCM-SHA256	STRONG
TLS13-AES-256-GCM-SHA384	STRONG
TLS13-CHACHA20-POLY1305-SHA256	STRONG
TLS13-AES-128-CCM-SHA256	SECURE
TLS13-AES-128-CCM-8-SHA256	SECURE

Table 23 includes that web applications that were HTTP only and do not have cipher tables above.

Table 23: HTTP Only Web Applications

HTTP Only

<Redacted>
<Redacted>
<Redacted>
<Redacted>
<Redacted>
<Redacted>
<Redacted>

Additional information about SSL best practices, ciphers strengths and testing utilities used to develop this analysis is detailed in **Table 24**.

Table 24: SSL Best Practices Resources

Description	URL
SSL Labs Best Practices	https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices
Open SSL to IANA Name matrix	https://testssl.sh/openssl-iana.mapping.html
Cipher Suite Strengths	https://ciphersuite.info/cs/?software=all&singlepage=true
External Website SSL Testing Utility	https://www.ssllabs.com/ssltest/
Internal Website SSL Testing Utility	<a href="https://github.com/<Redacted>zilla/cipherscan">https://github.com/<Redacted>zilla/cipherscan

Table 25 summarizes what SSL and TLS versions were found by the Nessus scanning engine during a scan of all ports of the infrastructure. Insecure versions of SSL and TLS were found on a number of systems and a range of ports. Red text is used to indicate versions of TLS and SSL that are deprecated and no longer meeting standard best practices.

Table 25: Infrastructure TLS Summary

System Name	IP Address	SSL 3.0	TLS 1.0	TLS 1.1	TLS 1.2	TLS 1.3
<Redacted>	<Redacted>	No	No	No	Yes	No
<Redacted>	<Redacted>	No	Yes	Yes	Yes	No
<Redacted>	<Redacted>	No	No	No	Yes	No
<Redacted>	<Redacted>	No	No	No	Yes	No
<Redacted>	<Redacted>	No	Yes	Yes	Yes	No
<Redacted>	<Redacted>	No	Yes	Yes	Yes	Yes

System Name	IP Address	SSL 3.0	TLS 1.0	TLS 1.1	TLS 1.2	TLS 1.3
<Redacted>	<Redacted>	No	Yes	Yes	Yes	No
<Redacted>	<Redacted>	No	Yes	Yes	Yes	Yes
<Redacted>	<Redacted>	No	Yes	Yes	Yes	No
<Redacted>	<Redacted>	No	No	No	Yes	No
<Redacted>	<Redacted>	No	No	No	Yes	No
<Redacted>	<Redacted>	No	No	No	Yes	No
<Redacted>	<Redacted>	No	No	No	Yes	No
<Redacted>	<Redacted>	No	Yes	Yes	Yes	No
<Redacted>	<Redacted>	Yes	Yes	Yes	No	No
<Redacted>	<Redacted>	No	Yes	Yes	Yes	No
<Redacted>	<Redacted>	No	Yes	Yes	Yes	No
<Redacted>	<Redacted>	Yes	Yes	No	No	No
<Redacted>	<Redacted>	No	Yes	No	No	No

2.3 Penetration and Exploitation Testing

Once BerryDunn identified potential vulnerabilities to exploit, we attempted to gain access to the <Redacted> internal network. Using tools such as Qualys Web Application Scanner, NMAP and Kali Linux, and Chrome’s Developer tools, a series of tests were performed; the following sections outline the results of the testing efforts.

BerryDunn completed a series of exploitation attempts against identified vulnerabilities in attempt to gain access to the internal network. **Table 26** provides a summary of the exploitation attempts and whether the exploitation attempt was successful.

Table 26: Summary of Exploitation Attempts

Exploitation Description	Exploit Target(s)	Status
SMB Enumerate Users <Redacted>	<Redacted>	Successfully identified local user accounts
SMBv1 EternalBlue Vulnerability	<Redacted>	SMBv1 was detected on <Redacted> Both systems were not vulnerable to the attack.
WebSphere Java Deserialization Vulnerability <Redacted>	<Redacted>	Session was not successfully created.

Exploitation Description	Exploit Target(s)	Status
WebSphere Snoop Servlet Information Disclosure	<Redacted>	Successful, information about the system was disclosed.
Tomcat CGI Servlet enableCmdLineArguments Vulnerability	<Redacted>	Unsuccessful
SNMP Enumeration	<Redacted>	Information about the environment was successfully disclosed.
Cross-Site (XSS) Scripting Vulnerabilities	<Redacted>	Multiple vulnerabilities were confirmed.
Blind SQL Injection Vulnerability	<Redacted>	One instance was detected.
Login form submitted in clear text	<Redacted>	Two instances detected.

2.3.1 Open Port Map

The first step in the test was to run an NMAP scan of the external-facing (public) IP range associated with <REDACTED>, the results of the NMAP scan produced the following port information. **Table 27** summarizes the ports that were found. All other ports were closed or filtered. These open ports should be reviewed, and any that are not strictly necessary for business requirements should be disabled.

Table 27: NMAP Discovery Results

IP Address	Open Ports
<Redacted>	21/open/tcp/ftp/, 22/open/tcp/ssh/, 80/open/tcp/http/, 111/open/tcp/rpcbind/, 1501/open/tcp/sas-3/, 2809/open/tcp/corbaloc/, 8222/open/tcp/unknown/, 9080/open/tcp/qlrpc/, 9<Redacted>0/open/tcp/jetdirect/
<Redacted>	21/open/tcp/ftp/, 22/open/tcp/ssh/, 80/open/tcp/http/, 135/open/tcp/msrpc/, 139/open/tcp/netbios-ssn/, 443/open/tcp/https/, 445/open/tcp/microsoft-ds/, 990/open/tcp/ftps/, 2001/open/tcp/dc/, 3389/open/tcp/ms-wbt-server/, 5120/open/tcp/barracuda-bbs/, 5432/open/tcp/postgresql/, 49153/open/tcp/unknown/, 49154/open/tcp/unknown/, 49155/open/tcp/unknown/, 49156/open/tcp/unknown/
<Redacted>	21/open/tcp/ftp/, 22/open/tcp/ssh/, 80/open/tcp/http/, 135/open/tcp/msrpc/, 139/open/tcp/netbios-ssn/, 443/open/tcp/https/, 445/open/tcp/microsoft-ds/, 990/open/tcp/ftps/, 2001/open/tcp/dc/, 3389/open/tcp/ms-wbt-server/, 5120/open/tcp/barracuda-bbs/, 49152/open/tcp/unknown/, 49153/open/tcp/unknown/, 49154/open/tcp/unknown/, 49155/open/tcp/unknown/, 49156/open/tcp/unknown/

IP Address	Open Ports
<Redacted>	21/open/tcp/ftp/, 22/open/tcp/ssh/, 80/open/tcp/http/, 81/open/tcp/hosts2-ns/, 111/open/tcp/rpcbind/, 389/open/tcp/ldap/, 443/open/tcp/https/, 1443/open/tcp/ies-lm/, 1501/open/tcp/sas-3/, 2049/open/tcp/nfs/, 8222/open/tcp/unknown/, 8400/open/tcp/cvd/, 9080/open/tcp/glrpc/, 9081/open/tcp/cisco-aqos/, 9<Redacted>0/open/tcp/jetdirect/, 9<Redacted>1/open/tcp/jetdirect/, 50000/open/tcp/ibm-db2/
<Redacted>	80/open/tcp/http/, 135/open/tcp/msrpc/, 139/open/tcp/netbios-ssn/, 445/open/tcp/microsoft-ds/, 3389/open/tcp/ms-wbt-server/, 8080/open/tcp/http-proxy/, 9998/open/tcp/distinct32/, 49152/open/tcp/unknown/, 49153/open/tcp/unknown/
<Redacted>	80/open/tcp/http/, 443/open/tcp/https/
<Redacted>	80/open/tcp/http/, 443/open/tcp/https/
<Redacted>	80/open/tcp/http/, 82/open/tcp/xfer/, 135/open/tcp/msrpc/, 139/open/tcp/netbios-ssn/, 445/open/tcp/microsoft-ds/, 3389/open/tcp/ms-wbt-server/, 5120/open/tcp/barracuda-bbs/, 32775/open/tcp/sometimes-rpc13/
<Redacted>	80/open/tcp/http/, 82/open/tcp/xfer/, 135/open/tcp/msrpc/, 139/open/tcp/netbios-ssn/, 445/open/tcp/microsoft-ds/, 3389/open/tcp/ms-wbt-server/, 5120/open/tcp/barracuda-bbs/, 32775/open/tcp/sometimes-rpc13/

2.3.2 Default Web Pages

BerryDunn then scanned ports 80 and 443 to determine web server behavior and the default landing pages. **Table 28** catalogs the default pages discovered and the HTTP/HTTPS behavior seen on each site. A number of default product pages were observed, including default Internet <Redacted>. Default web pages can indicate an unused and unpatched web server, which may be used by an attacker as an entry point. In addition, login pages were discovered that did not utilize HTTPS for securely transmitting credentials.

Table 28: Default Web Page Discovery

Default Landing Pages	Systems
<Redacted>	<Redacted>
<Redacted>	<Redacted>
<Redacted>	<Redacted>
<Redacted>	<Redacted>
<Redacted>	<Redacted>
<Redacted>	<Redacted>
<Redacted>	<Redacted>
<Redacted>	<Redacted>

Default Landing Pages	Systems
<Redacted>	<Redacted>

2.3.3 Server Message Block (SMB) Exploits

Next, we attempted to exploit vulnerabilities discovered as part of scanning.

The first exploit was to leverage NMAP Scripting Engine's (NSE) SMB-Enum-Users script against <Redacted>, as shown in **Exhibit A**.

Exhibit A: NSE: SMB-Enum-Users

<Redacted>

Exhibit B illustrates the response received from the server. The system is configured to allow any<Redacted>us lookups of the host security identifier (SID). With the host SID, an attacker can enumerate the local users on the system. By getting a list of who has access to it, the attacker might get a better idea of what to target (if financial people have accounts, it probably relates to financial information). Additionally, knowing which accounts exist on a system (or on multiple systems) allows the attacker to build a dictionary of possible usernames for brute force attacks, such as a SMB brute force or a Telnet brute force. These accounts may be helpful for other purposes, such as using the accounts in Web applications on this or other servers.

Exhibit B: SMB Enumerate Users Response

<Redacted>

BerryDunn attempted to detect if a Microsoft SMBv1 server is vulnerable to a <Redacted> code execution vulnerability (ms17-0<Redacted>, a.k.a. EternalBlue). The vulnerability is actively exploited by WannaCry and Petya ransomware and other malware. SMBv1 was detected on <Redacted> and <Redacted>. Both were not vulnerable. **Exhibit C** shows the responses received by the Metasploit <Redacted>.

Exhibit C: SMBv1 EternalBlue Vulnerability

<Redacted>

2.3.4 WebSphere Exploits

BerryDunn next attempted to exploit a vulnerability in IBM's WebSphere Application Server against target <Redacted>. An unsafe deserialization call of unauthenticated Java objects exists to the Apache Communications Collections (ACC) library, which allows re<Redacted>te arbitrary code execution. Authentication is not required in order to exploit this vulnerability.

Exhibit D documents that this was not successful.

Exhibit D: WebSphere Java Deserialization Vulnerability

<Redacted>

Next, the penetration testing team attempted to gain information from WebSphere. This script attempts to enumerate the actual physical path of the servlet classes by requesting a version of 'snooservlet' which is missing required classes. **Exhibit E** demonstrates the information acquired from the 'snooservlet' request. An attacker, gaining information about the actual physical layout of the file system, can use the information in crafting <Redacted> complex attacks. If not required, uninstall the default applications.

Exhibit E: WebSphere Snoop Information Disclosure

<Redacted>

2.3.6 SNMP Exploits

The BerryDunn testing team used SNMP to gather information from a system <Redacted> in the environment, demonstrated in **Exhibit G**. The system utilizes the default, well known community string of "public", which allows easy access to information about the system.

Exhibit F: SNMP Enumeration

<Redacted>

Table 29 illustrates some of the information that could be disclosed to an attacker. The information disclosure of active connections to other systems could be useful to an attacker in crafting additional attacks.

Table 29: SNMP Information Disclosure

Category	Data
<Redacted>	<Redacted>
<Redacted>	<Redacted>
<Redacted>	<Redacted>
<Redacted>	<Redacted>

2.3.7 Cross-Site Scripting (XSS)

A number of XSS vulnerabilities were discovered in the web applications tested. If the user-supplied data contain characters that are interpreted as part of an HTML element instead of literal text, then an attacker can <Redacted> modify the HTML that is received by the victim's web browser.

The XSS payload is echoed in HTML document returned by the request. An XSS payload may consist of HTML, JavaScript, or other content that will be rendered by the browser. In order to exploit this vulnerability, a malicious user would need to trick a victim into visiting the URL with the XSS payload.

XSS exploits pose a significant threat to a web application, its users, and user data. XSS exploits target the users of a web application rather than the web application itself. An exploit can lead to theft of the user's credentials and personal or financial information.

All data collected from the client should be filtered, including user-supplied content and browser content such as Referrer and User-Agent headers. **Table 30** lists the instances of XSS that were discovered during BerryDunn's testing.

Table 30: Instances of Cross-Site Scripting Vulnerabilities

URL	Parameter
<Redacted>	screenname
<Redacted>	providerType
<Redacted>	q
<Redacted>	archiveFileSearch
<Redacted>	archiveFileSearch
<Redacted>	showLayouts

Exhibit H documents one example of one of the XSS vulnerabilities detected. Highlighted in red is the URL and parameter that was vulnerable. Also highlighted is the payload that was sent to the web server, and the payload reflected back in the server's response.

Exhibit G: Cross-Site (XSS) Scripting Vulnerability

<Redacted>

2.3.8 Blind SQL Injection

Blind SQL injection is a specialized type of SQL injection that enables an attacker to modify the syntax of a SQL query in order to retrieve, corrupt, or delete data. A successful exploit manipulates the query's logic. Queries created by concatenating strings with SQL syntax and user-supplied data are prone to this vulnerability. When any part of the string concatenation can be modified, an attacker has the ability to change the meaning of the query.

Typical detection techniques for SQL injection vulnerabilities use a payload that attempts to produce a SQL error from the web application. Detection based on blind SQL injection uses inference based on the differences <Redacted> the application's responses to various payloads. A well-known technique called True / False inference to determine if there is a blind SQL injection vulnerability. Two conditions are tested: one with a True condition and another with a False condition. If there is a blind SQL injection vulnerability, the query with the True condition payload will cause the web application to return a different response than the false condition payload.

When a difference occurs, the conclusion is that there is a blind SQL injection vulnerability. **Exhibit I** shows the details of the blind SQL injection that was discovered.

The scope of a SQL injection exploit varies greatly. If any SQL statement can be injected into the query, then the attacker has the equivalent access of a database administrator. This access could lead to theft of data, malicious corruption of data, or deletion of data.

SQL injection vulnerabilities can be addressed in three areas: input validation, query creation, and database security. All input received from the client side should be validated for correct content. If a value's type or content range is known beforehand, then stricter filters should be applied. Prepared statements (also referred to as parameterized queries) provide strong protection from SQL injection. Prepared statements are precompiled SQL queries whose parameters can be modified when the query is executed. These functions are more secure than string concatenation for assigning user-supplied data to a query.

Exhibit H: Blind SQL Injection Vulnerability

<Redacted>

2.3.9 Insecure Login Forms

Two login forms were identified where the default action contains a link that is not submitted via HTTPS (HTTP over SSL). Sensitive data such as authentication credentials should be encrypted when transmitted over the network. **Table 31** details the forms that were discovered.

Table 31: Instances of Insecure Login Forms

URL
<Redacted>
<Redacted>

Exhibit J illustrates one of the login forms that was detected.

Exhibit I: Login Form Not Submitted over HTTPS

<Redacted>

2.4 .NET Framework Information

As a part of BerryDunn's vulnerability scanning of the <REDACTED> Windows environment, multiple versions of .NET Framework were detected within the environment including:

- 2.0.50727
- 3.0
- 3.5

- 4.6.2
- 4.7
- 4.7.2
- 4.8

Some systems had multiple .NET versions installed on them simultaneously. The .NET Framework was designed to allow multiple versions to be installed on a system and used at the same time without conflict. Other systems failed to return any information related to the .NET Framework. This may indicate that these systems do not have .NET installed, but this has not been verified.

One of the primary areas of concern related to the older versions of the .NET Framework involves an exploit of deserialization in ASP.NET through the use of ViewState. ViewState is a base64 serialized parameter used in ASP.NET to help preserve the current webpage and persist any non-default information (such as user inputs into a form) during a POST request. This parameter would be deserialized when received by the server to receive the data. The vulnerability allows remote code execution on the web server if the ViewState is forged. This is possible when the MAC validation feature is disabled in ViewState; with knowledge of the validation key and algorithm in .NET versions prior to version 4.5; or by knowing the validation key validation algorithm, decryption key, and decryption algorithm in version 4.5 and above.

In order to prevent this type of an exploit, some mitigation methods include:

- Upgrading the .NET Framework in use to a version where MAC validation cannot be disabled, which includes version 4.5 or higher.
- Ensure that the MachineKey pages of configuration files (web.config or machine.config) are generating keys dynamically at runtime instead of having them hardcoded.
- Encrypt any sensitive parameters included in configuration files.
- Using the ViewStateUserKey property on applicable pages can help to prevent Cross-Site Request Forgery.
- Ensure that any disclosed validation or decryption keys are regenerated.
- Ensure that custom error pages are in use to prevent users from seeing any of the actual .NET error messages.

Table 32 provides the details of the .NET version and installation data found by system. The table includes red text for areas of potential concern, whether this be because of an older version of .NET in use or because it is unknown if .NET is in use on that server from testing.

Table 32: .NET Versions and Installation Data

Name / IP	OS Version	.NET Versions Detected
<Redacted>	Microsoft Windows Server 2019 Standard	Path : C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ Version : 4.7.2 Full Version : 4.7.03190 Install Type : Full Release : 461814 Path : C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ Version : 4.7.2 Full Version : 4.7.03190 Install Type : Client Release : 461814
<Redacted>	Microsoft Windows Server 2019 Standard	No information returned by scanner, not installed by default on Server 2019
<Redacted>	Microsoft Windows Server 2019 Standard	Path : C:\Windows\Microsoft.NET\Framework64\v2.0.50727 Version : 2.0.50727 Full Version : 2.0.50727.4927 SP : 2 Path : C:\Windows\Microsoft.NET\Framework64\v3.0 Version : 3.0 Full Version : 3.0.30729.4926 SP : 2 Path : C:\Windows\Microsoft.NET\Framework64\v3.5\ Version : 3.5 Full Version : 3.5.30729.4926 SP : 1 Path : C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ Version : 4.7.2 Full Version : 4.7.03190 Install Type : Full Release : 461814 Path : C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ Version : 4.7.2

Name / IP	OS Version	.NET Versions Detected
		Full Version : 4.7.03190 Install Type : Client Release : 461814
<Redacted>	Microsoft Windows Server 2019 Standard	No information returned by scanner, not installed by default on Server 2019
<Redacted>	Microsoft Windows Server 2019 Standard	No information returned by scanner, not installed by default on Server 2019
<Redacted>	Microsoft Windows Server 2019 Standard	Path : C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ Version : 4.7.2 Full Version : 4.7.03190 Install Type : Full Release : 461814 Path : C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ Version : 4.7.2 Full Version : 4.7.03190 Install Type : Client Release : 461814
<Redacted>	Microsoft Windows Server 2019 Standard	Path : C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ Version : 4.7.2 Full Version : 4.7.03190 Install Type : Full Release : 461814 Path : C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ Version : 4.7.2 Full Version : 4.7.03190 Install Type : Client Release : 461814