




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 2

[List View](#)**General Information** | [Contact](#) | [Default Values](#) | [Discount](#) | [Document Information](#) | [Clarification Request](#)

Procurement Folder: 1369290

Procurement Type: Central Master Agreement

Vendor ID: 000000177557 


Legal Name: ERNST &amp; YOUNG LLP

Alias/DBA:

Total Bid: \$117,000.00

Response Date: 03/28/2024 

Response Time: 13:17

Responded By User ID: 000000177557 

First Name: Draunta

Last Name: Dorsey

Email: draunta.dorsey@ey.com

Phone: 3043438971

SO Doc Code: CRFQ

SO Dept: 0705

SO Doc ID: LOT2400000009

Published Date: 3/21/24

Close Date: 3/28/24

Close Time: 13:30

Status: Closed

Solicitation Description: Network Penetration Testing and Cybersecurity Assessments

Total of Header Attachments: 2

Total of All Attachments: 2



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

**State of West Virginia  
 Solicitation Response**

<b>Proc Folder:</b>	1369290	
<b>Solicitation Description:</b>	Network Penetration Testing and Cybersecurity Assessments	
<b>Proc Type:</b>	Central Master Agreement	
<b>Solicitation Closes</b>	<b>Solicitation Response</b>	<b>Version</b>
2024-03-28 13:30	SR 0705 ESR03282400000005557	1

<b>VENDOR</b>
000000177557 ERNST & YOUNG LLP

**Solicitation Number:** CRFQ 0705 LOT2400000009  
**Total Bid:** 117000      **Response Date:** 2024-03-28      **Response Time:** 13:17:27  
**Comments:**

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

<b>Vendor Signature X</b>	<b>FEIN#</b>	<b>DATE</b>
---------------------------	--------------	-------------

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

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
1	External Network Penetration Testing				24000.00

Comm Code	Manufacturer	Specification	Model #
81111801			

**Commodity Line Comments:** Estimated Travel expenses: \$11,000 - Total of \$128,000

**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				24000.00

Comm Code	Manufacturer	Specification	Model #
81111801			

**Commodity Line Comments:**

**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				46000.00

Comm Code	Manufacturer	Specification	Model #
81111801			

**Commodity Line Comments:**

**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				23000.00

Comm Code	Manufacturer	Specification	Model #
81111801			

**Commodity Line Comments:**

**Extended Description:**

See Attached Specifications and Exhibit - A Pricing Page

# West Virginia State Lottery

Security Testing Services

March 2024







Ernst & Young LLP  
5 Times Square  
New York, NY, 10036

Tel: +1 (212) 773 3000  
Fax: +1 (212) 773 6350  
ey.com

March 28, 2024

**Brandon Barr**  
West Virginia State Lottery  
2019 Washington St, East  
Charleston, WV 25305

Dear Brandon,

Thank you for the opportunity to support West Virginia State Lottery in assessing its cybersecurity defenses. We are confident that EY is distinctly qualified to support you with this important initiative. To assist you in meeting your objectives, we have assembled a team with relevant industry experience, deep technical knowledge and unique understanding of your organization and key areas of focus. We understand this is an important topic and focus area for your executive management team . As one of the largest providers of cyber related consulting services in the world, we have completed hundreds of assessments for similar sized organizations. Further, we are not only an assessor, we possess the practical skills and experience to help you prioritize and implement tangible improvements that will improve your organization’s security posture.

Our proposal highlights our approach for delivering on your desired outcomes incorporating these key attributes:

- **A leader in cybersecurity** : With a proven methodology and tools, culture of knowledge sharing and collaboration, and a risk-based approach to security, EY is recognized as a leader in cybersecurity. Globally, we have more than 7,000 cybersecurity and risk management professionals holding recognized certifications. Our qualified professionals deliver specific technical experience and leading practices to provide you with you with fresh perspectives, objectivity and help in managing your risks while improving your business.
- **Deep penetration testing experience** — Our team includes in-house security engineers that reside in our world-class dedicated Advanced Security Center (ASC). Our teams conduct several hundred attack and penetration assessments globally every year including Gaming & Betting Industry clients as well as companies listed on the Global Fortune 500 list. This experience will help us identify key vulnerabilities in your environment, and provide actionable recommendations for remediation.
- **Access to a broad network of subject matter resources that we can match to the needs of the project:** Because of our size, we have the benefit of housing a broad range of skills and capabilities in the Cybersecurity assessment space. Our Cybersecurity assessment teams bring a multitude of leading practice knowledge and experience in this domain in working across large and complex organizations.
- **Quality, independence, and objectivity, available to you in a cost-effective and efficient way:** Our commitment to West Virginia State Lottery is to provide you with the highest level of quality service and transparency. We take pride in delivering work to last the test of time while providing you with a fair and transparent fee schedule.

We look forward to the opportunity to work with you on this important initiative and are ready to begin supporting you as soon as a decision is made. Please feel free to reach out John Leo directly at 201.551.5007 or john.leo@ey.com should you have any questions or points for clarification.

Sincerely,

**John Leo, Jr.**  
EY | Managing Director  
john.leo@ey.com



# Table of contents

01	Executive summary	3
02	Our approach, methodology and framework	4
03	Our work products	15
04	Engagement Fees, Assumptions and Team	17
05	Why EY?	19



# Executive summary

## Our understanding of your needs

- Perform External, Internal and Web assessment and Wireless testing to identify potential weaknesses in West Virginia State Lottery’s cyber defenses and assess their resilience via a combination of attack vectors including external, remote access/social engineering , intranet, wireless.
- Provide advice and recommendations to remediate or mitigate the vulnerabilities present in the in-scope systems and applications
- Collaboratively work with West Virginia State Lottery during the course of the assessment to provide detection and response insights

## How our approach and capabilities benefit you

- Our business-focused approach balances cost versus value to identify and protect the right information assets that align with your business risk appetite.
- Our dedicated Advanced Security Centers (ASC) have conducted a wide range of attack and penetration assessments across different industries, from infrastructure testing to red/purple team assessment. Our team brings experience in network architecture, compliance requirements and OT.
- With a proven methodology and tools, a culture of knowledge-sharing and collaboration, and a risk-based, business-centric approach to security, we are consistently recognized as a leader in cybersecurity by Forrester, Gartner, Security Ventures, IDC MarketScape and independent organizations.

## Resulting value to West Virginia Lottery

- A risk-based approach on protecting your information assets against vulnerabilities and threats.
- Collaboration during the assessment to timely report critical vulnerabilities that requires immediate responses to protect West Virginia State Lottery from real threat actors.
- Effective communication of vulnerabilities, impact and recommendations to executive sponsors and technical stakeholders by appropriate levels of team members and experiences.
- Collaboration post-assessment to review vulnerabilities and exploitation techniques as well as to provide insights into West Virginia State Lottery’s detection and response capabilities.

## Why EY?

### Experienced team

Our dedicated Advanced Security Centers (ASC) located strategically across the globe have conducted security assessments in the different industries, from external threat landscape assessments to malware simulations and red teaming. Our team brings experience in business contexts and cybersecurity to support you in meeting the organization’s objectives.



### Industry knowledge

We will leverage our institutional knowledge of your industry and past penetration testing experience by bringing subject matter resources to help navigate through the complexities of your environment. Our team of cybersecurity professionals will be guided by EY leaders who are most familiar with your business and objectives.



### Strong cybersecurity brand

- Dedicated Cybersecurity practice
- Leaders for GCC Professional Security Services by 2020 IDC MarketScape
- Ranked #1 by Cybersecurity Ventures
- Winner of Biohacking Village CTF at Defcon 2019 and 2022
- Ranked #2 in a Cloud CTF challenge at Defcon 2022







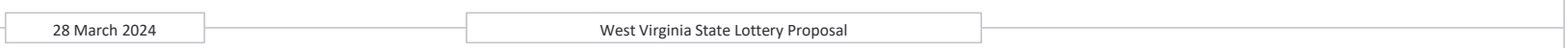
## Our approach, methodology and framework

# Our approach

The engagement is divided into four phases as shown below.



	Project planning	Assessment	Reporting
<b>Activities</b>	<p>EY will collaborate with West Virginia State Lottery to agree on rules of engagement, plan and logistics. Based on initial discussion, the scope of work will consist of the potential threat scenarios:</p> <ol style="list-style-type: none"> <li>External threat actors with limited knowledge of West Virginia State Lottery's IT environment</li> <li>Identifying and enumerating assets to determine safe, controlled testing of the target environment while meeting test objectives without adversely impacting West Virginia State Lottery.</li> </ol> <p>Additionally, EY will work with West Virginia State Lottery to identify the list of the vulnerabilities for regression testing.</p>	<p><u>External Penetration Testing and Social Engineering</u> — Perform an assessment of West Virginia State Lottery's external presence to identify and exploit vulnerabilities of West Virginia State Lottery's Internet facing system and network that could lead an attacker to gain access to West Virginia State Lottery's corporate network. A component of this assessment will include a phishing exercise that will target employees gathered through open-source intelligence (OSINT) and to be verified by West Virginia State Lottery.</p> <p><u>Internal Penetration Testing</u> — Perform an assessment on West Virginia State Lottery's internal network, including servers, workstations, databases, trusted/accessible environments, and other network devices to identify and exploit vulnerabilities. Tests will be conducted from the perspective of an assumed breach/insider-threat actor with the objective of achieving the agreed upon objectives as follows:</p> <ul style="list-style-type: none"> <li>Identify and gain unauthorized access to Privileged Access Management (PAM) solutions</li> <li>Identify and gain authorized access to enterprise backup solutions</li> <li>Obtain Domain Administrator access and attempt cross-domain access to restricted environments</li> <li>Move laterally between different Active Directory domains within the forest(s)</li> </ul> <p><u>Web Application Testing</u> – EY evaluates the current standards of your internal or commercial enterprise applications against industry benchmarks and provides a well-developed matrix of existing threats and vulnerabilities in your applications as well as recommendations to address specific weaknesses.</p> <p><u>Wireless penetration Testing</u> — EY will perform penetration testing against West Virginia State Lottery's wireless infrastructure to evaluate the security controls surrounding wireless systems. During our testing we will attempt to identify vulnerabilities that would allow access to West Virginia State Lottery internal systems. Some of these activities include:</p> <ul style="list-style-type: none"> <li>Identifying weak encryption</li> <li>Detect poorly configured access points</li> <li>Rogue access points / Evil twin attacks</li> </ul>	<p>After test completion, EY will document the results of all tests and develop a detailed report capturing findings and recommendations based upon the strengths and gaps identified.</p> <p>EY will deliver two formal executive presentations to West Virginia State Lottery's senior management.</p>
<b>Work products</b>	<ul style="list-style-type: none"> <li>Confirm plan and approach</li> <li>Scope restrictions and rules of engagement</li> </ul>	<ul style="list-style-type: none"> <li>Status updates</li> <li>Test results and findings</li> <li>Critical escalations (if needed)</li> <li>Confirmation of enumerated OT assets and planning for target selection activities and metrics for satisfying</li> </ul>	<ul style="list-style-type: none"> <li>Weekly status updates</li> <li>Findings presentation</li> </ul>

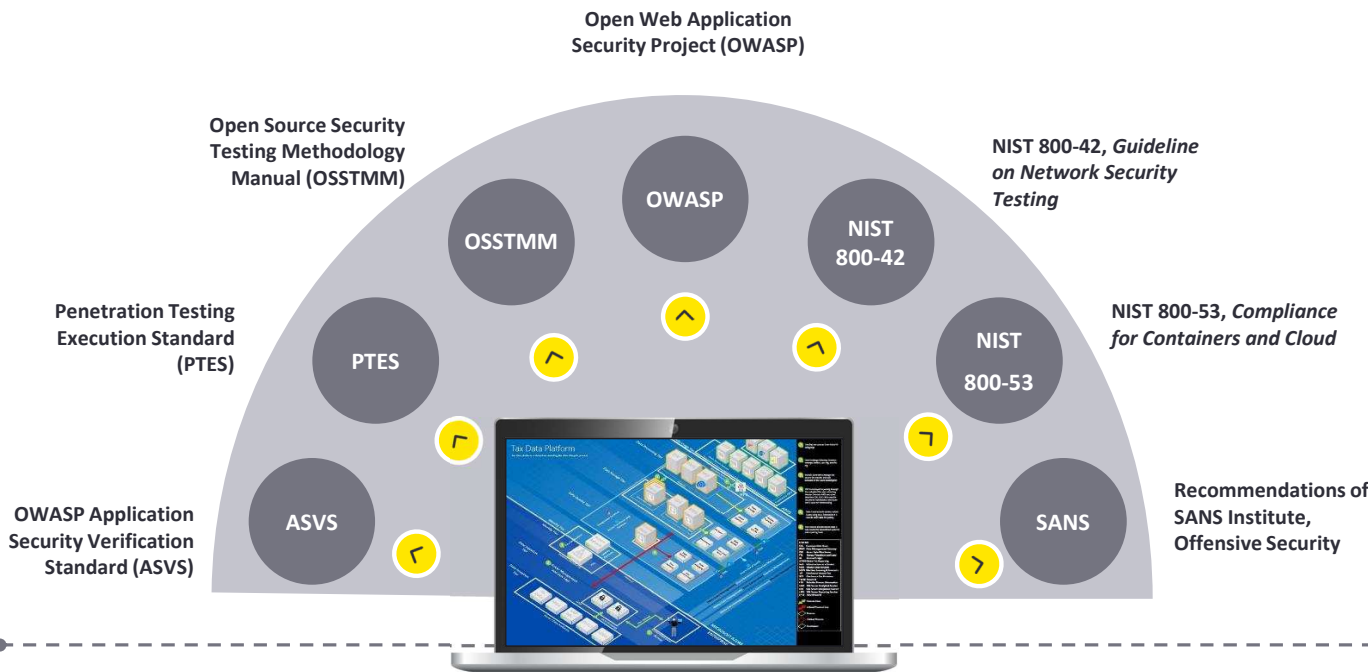


# Penetration Testing Standards and Frameworks

We have developed a methodology for penetration testing that is based on extensive international experience in delivering similar exercises. It is consistent with the best practices in this area and uses, among others, proven elements of the following methodologies and studies:

## Key features of our approach

- Global reach and coverage
- Tried-and-tested approach working successfully for other global firms
- Flexible and can be tailored to your needs
- Coverage across all test types
- Certified penetration testers with experience on many similar engagements
- Detailed and summary reporting for each test which is concise and can be used to drive remediation activities
- Defined stages for ease of reporting, tracking and improving efficiency



28 March 2024

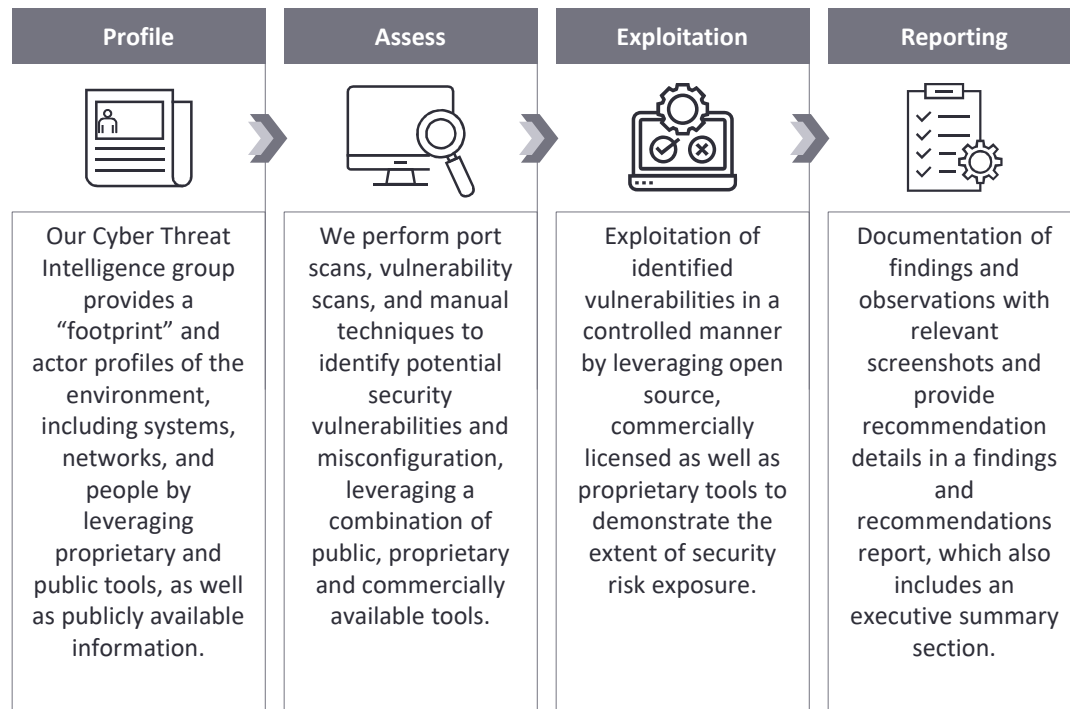
West Virginia State Lottery Proposal



# Our attack and penetration testing methodology applied

## Attack and penetration assessment

Our approach leverages the collective knowledge EY has gained from performing several hundred penetration assessments every year. Our methodology is designed to identify exploitable vulnerabilities specific to your environment EY that would allow us to outline the impact on what matters to you. Our approach is represented by the following framework:



### Differentiators

**Automation and custom tooling**

- Combination of commercial, open source and proprietary tools
- Toolset selected to emulate real-world threats

**Human skills driven by threat intel**

- Extensive hands-on experience
- Emphasis on manual testing to pivot like a real world attacker
- Focus on “real life” exploitation and vulnerability linkage

**Customized test plans and reports**

- Flexible methodology
- Understanding of needs and priorities
- Customization of activities and test phases to each environment



# External network penetration testing methodology

EY will perform an external network penetration test of West Virginia State Lottery’s systems and technology connected to and accessible through the public Internet. EY will perform this as a “zero knowledge” test, identifying IP range information through publicly available resources.



	<b>Profile</b> Gather information and identify targets performing a “zero knowledge” or “limited knowledge” approach test	<b>Assess</b> Programmatically scan the ranges/addresses using public, proprietary and commercially available tools	<b>Exploit</b> Obtain access to targets and evaluate the impact of potential vulnerabilities
<b>Key activities</b>	<ul style="list-style-type: none"> <li>Enumerate network by querying American Registry for Internet Numbers (ARIN), and other databases</li> <li>Identify domains and sub domains</li> <li>Utilize Shodan and Censys to identify additional hosts</li> <li>Enumerate the network through Whois information</li> <li>Query DNS to discover additional hosts</li> <li>Evaluate service/system availability through Denial of Service (DOS) on in-scope systems.</li> </ul>	<ul style="list-style-type: none"> <li>Perform network service and port scans to identify accessible services running on the target IP addresses</li> <li>Perform automated vulnerability scans to identify vulnerabilities, e.g., unauthorized access, missing security patches, weak or default credentials in use, misconfigured network services and exposed sensitive data</li> <li>Analyze &amp; assess output from the scan</li> </ul>	<ul style="list-style-type: none"> <li>Perform In-depth penetration testing of in-scope systems to assess the impact of potential vulnerabilities</li> <li>Attempt exploitation of high-risk potential vulnerabilities to validate exploitability</li> <li>Leverage exploited vulnerabilities in attempts to gain access to additional systems</li> </ul>
<b>Output</b>	<ul style="list-style-type: none"> <li>Results of network ranges, domains, hosts, and system availability.</li> </ul>	<ul style="list-style-type: none"> <li>Results of vulnerability scans</li> <li>Preliminary list of possible vulnerabilities</li> <li>Potential exploitation paths</li> </ul>	<ul style="list-style-type: none"> <li>Immediate notification of critical risk issues</li> <li>Exploitation path</li> </ul>



Weekly status update meetings





# Internal network penetration testing methodology

EY will perform an internal network penetration test on West Virginia State Lottery’s internal network, including servers, workstations, and other network devices available through West Virginia State Lottery’s internal environment. The assessment will be performed with an objective of identifying vulnerabilities and escalating privileges.



	<b>Profile</b> Gather information and identify targets performing a “zero knowledge” or “limited knowledge” approach test	<b>Assess</b> Programmatically scan the IP ranges/addresses using public, proprietary and commercially available tools	<b>Exploit</b> Obtain access to targets and evaluate the impact of potential vulnerabilities
<b>Key activities</b>	<ul style="list-style-type: none"> <li>Enumerate network within the in-scope target environment</li> <li>Interrogate DNS to discover additional related hosts</li> <li>Identify live hosts</li> <li>Identify operating system and application fingerprint</li> <li>Identify network policies and settings</li> </ul>	<ul style="list-style-type: none"> <li>Analyze network traffic and assess services and protocols in use</li> <li>Perform services and vulnerability scans</li> <li>Identify misconfigured services and insecure configuration</li> <li>Perform password guessing, cracking, credential reuse, pass the hash techniques</li> <li>Conduct internal attacks to compromise hosts, applications, move laterally and escalate privileges to administrator level</li> </ul>	<ul style="list-style-type: none"> <li>Perform manual validation of identified issues</li> <li>Link vulnerabilities and attempt exploitation</li> <li>Leverage access to elevate privileges across network</li> </ul>
<b>Output</b>	<ul style="list-style-type: none"> <li>List of identified West Virginia State Lottery’s assets.</li> <li>Mapping of internal footprint</li> </ul>	<ul style="list-style-type: none"> <li>Results of vulnerability scans</li> <li>Preliminary list of possible vulnerabilities</li> <li>Potential exploitation paths</li> </ul>	<ul style="list-style-type: none"> <li>Immediate notification of critical risk issues</li> <li>Exploitation path</li> </ul>



Weekly status update meetings

# Web applications penetration testing methodology

EY will evaluate the current standards of your web applications against industry best practices such as Open Web Application Security Project (OWASP) to identify security vulnerabilities and provide recommendations for specific weaknesses identified.



	<b>Profile</b> Enumerate application and identify functionalities performing a "zero knowledge" or "limited knowledge" approach test	<b>Assess</b> Identify potential security exposures through automated and manual testing	<b>Exploit</b> Attempt to exploit identified application vulnerabilities
<b>Key activities</b>	<ul style="list-style-type: none"> <li>Explore both unauthenticated and authenticated portions of the application</li> <li>Create a functionality map by crawling the application and exploring the live instance</li> <li>Log every request and response during this stage for analysis using a local proxy tools</li> </ul>	<ul style="list-style-type: none"> <li>Test the web application emulating a threat actor without credentials, as well as authenticated user roles</li> <li>Perform fuzzing and security testing of all the inputs fields</li> <li>Scan application for authentication, authorization and accounting (AAA) vulnerabilities</li> <li>Review and validate scan results manually to eliminate false positives</li> </ul>	<ul style="list-style-type: none"> <li>Perform manual test for common vulnerability categories within OWASP Top 10 list, such as authentication, misconfiguration, session management and other injections attacks (e.g., SQLi, XXS, OS cmd injection)</li> <li>Exploit broken access control issues to perform privilege escalation attacks</li> <li>Attempt exploitation of identified vulnerabilities</li> </ul>
<b>Output</b>	<ul style="list-style-type: none"> <li>Spreadsheet of discovery results</li> </ul>	<ul style="list-style-type: none"> <li>Results of scans</li> <li>Preliminary list of possible vulnerabilities</li> </ul>	<ul style="list-style-type: none"> <li>Immediate notification of critical risk issues</li> </ul>
Weekly status update meetings			



28 March 2024

West Virginia State Lottery Proposal



# Social engineering penetration testing methodology

EY's offers a range of expert-driven social engineering assessments designed to target and take advantage of the unpatchable exploit — the human-element, to gain access to your network.



<b>Profile</b> Create a social engineering profile of the organization's internet footprint, employee information and work culture	<b>Assess</b> Develop sophisticated social engineering campaigns based on threat modelling best suited for your organization	<b>Exploit</b> Obtain access to internal network and evaluate the impact of potential vulnerabilities
---	---	--

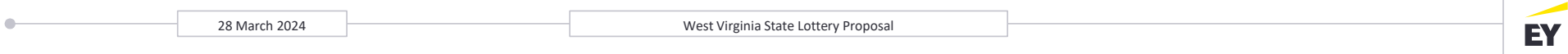
## Key activities

<ul style="list-style-type: none"> <li>Harvest information from publicly available sources to identify potential web portals for social engineering attacks</li> <li>Utilize OSINT tactics to gather organization-specific information such as employee names, email address, phone numbers, social media accounts and third party associations</li> </ul>	<ul style="list-style-type: none"> <li>Design deceptive phishing scenarios or voice call scripts that raise human interest</li> <li>Develop custom malwares to bypass security controls and gain internal network access</li> <li>Select targets for social engineering attack</li> </ul>	<ul style="list-style-type: none"> <li>Execute social engineering techniques</li> <li>Persuade employees to perform pre-determined actions</li> <li>Attempt exploitation</li> <li>Escalate privileges</li> <li>Document observations, findings and recommendations</li> </ul>
--	---	---

## Output

<ul style="list-style-type: none"> <li>List of web portals that can be targeted for phishing attacks</li> <li>Employee names, emails, job titles and phone numbers</li> </ul>	<ul style="list-style-type: none"> <li>Checkpoints after each step to communicate plan, activities and progress</li> </ul>	<ul style="list-style-type: none"> <li>Exploitation path</li> <li>Immediate notification of critical risk issues</li> </ul>
---	--	---

Weekly status update meetings



# Wireless penetration testing methodology

EY's wireless penetration testing methodology emulates an attacker attempting to gain access to your internal network through the wireless network, but also includes some elements of an audit, ensuring your wireless network is in-line with industry standards.



	<b>Profile</b> Gather information on wireless frequencies emanating from a target area and locate wireless access points	<b>Assess</b> Identify legitimate access point belonging to the organization and hunt for rogue access points	<b>Exploit</b> Attempt to exploit identified wireless networks to evaluate the impact of potential vulnerabilities
<b>Key activities</b>	<ul style="list-style-type: none"> <li>Discover wireless network (war-walk)</li> <li>Search for wireless radio frequency emanations, including 802.11a/b/g/n, using wireless network scanning tools</li> <li>Identify in-use wireless security suites e.g., authentication, data encryption, access controls</li> </ul>	<ul style="list-style-type: none"> <li>Identify the vendor, model of each access point and known vulnerabilities</li> <li>Identify wireless security weaknesses regarding authentication and data encryption (e.g., WEP, WPA, WPA2)</li> <li>Review network access controls between wireless network and other internal network segments</li> <li>Detect potential unauthorized access points</li> </ul>	<ul style="list-style-type: none"> <li>Attempt to compromise wireless security</li> <li>Attempt bypass network access control</li> <li>Attempt to gain unauthorized access to the internal network</li> <li>Attempt to compromise in-scope systems and networks</li> </ul>
<b>Output</b>	<ul style="list-style-type: none"> <li>List of identified wireless networks and access points</li> </ul>	<ul style="list-style-type: none"> <li>Results of analysis of each wireless network</li> <li>List of potential rogue access points and locations</li> </ul>	<ul style="list-style-type: none"> <li>Exploitation path</li> <li>Immediate notification of critical risk issues</li> </ul>



Weekly status update meetings

# EY's Vulnerability Assessment Process

## Discover

- Scan is a method used to find the assets on your network without scanning them for vulnerabilities. Preform Reconnaissance, this scan is helps collect an understanding of the assets on your network. The systems discovered move to the next phase of scanning for vulnerability detection.

## Prioritize

- Prioritizing vulnerabilities is a critical aspect of effective vulnerability management. Not all vulnerabilities pose the same risk, and limited resources may prevent organizations from addressing every vulnerability immediately. Prioritization helps us focus efforts on mitigating the most critical vulnerabilities first.

## Assess

- Assessment process takes place, leveraging vulnerabilities severity (base on CVSS and severity ranking). The risk of vulnerabilities are assessed taking in consideration asset information attributed.

## Report

- Once scans are complete, prioritization and assessments are conducted a report will be generated to provide detailed summary of the host, vulnerability, and remediation.

## Remediate

- We provide recommended remediation plans and rationalize treatment activity.

## Validate

- Validate updates/patches and support deployment to IT systems to remediate vulnerabilities





# Internal Network Vulnerability Assessment Methodology



	Initialization Define scope and understand current state	Assessment Perform discovering scanning of all in-scope assets	Summary and Reporting Document results of the assessment and findings
Key activities	<ul style="list-style-type: none"> <li>Obtain necessary access to perform agreed-upon activities</li> <li>Launch a host discovery scan to identify hosts on your network, and associated information such as IP address, FQDN, operating systems, and open ports, if available</li> <li>Conduct interviews to understand current state as needed</li> </ul>	<ul style="list-style-type: none"> <li>Conduct internal vulnerability scanning of the in-scope devices</li> <li>Verify vulnerability scan results extracted into vulnerability lifecycle management platform for completeness and data accuracy</li> <li>Analyze identified vulnerabilities, apply mutually agreed upon prioritization criteria to identify areas of high risk, and suggest remediation tasks</li> </ul>	<ul style="list-style-type: none"> <li>Document observations, findings and recommendations</li> <li>Provide recommendations for remediation prioritization based on business requirements and associated risks</li> </ul>
Output	<ul style="list-style-type: none"> <li>Scope definition for internal vulnerability scanning</li> <li>Understanding of target state in alignment with desired level of maturity and risk appetite</li> </ul>	<ul style="list-style-type: none"> <li>Scan reports and analysis of internal vulnerabilities</li> <li>Provide operational-level reporting for trending and aging analysis</li> </ul>	<ul style="list-style-type: none"> <li>Executive summary report with an overview of observations/findings, including scope, approach, testing results and recommendations</li> <li>Technical analysis report</li> </ul>
Weekly status update meetings			





Our work products

# Illustrative sample work products

At the conclusion of the engagement, you will receive a findings and recommendations report consisting of an executive summary and a detailed technical section.

## Executive Summary

### Introduction

Ernst & Young (EY) performed a red team attack and penetration assessment using real-life scenarios to determine COMPANY's ability to complicate, detect and respond to specific cyber threats.

The results of that assessment are contained within the details of this report and document the results from our attempts to leverage various testing approaches in conjunction with one another during simulated real-world attack scenarios as defined within the project's scope. The exploitation activities performed during this review demonstrate the different attack paths an adversary can successfully use to capture defined targets and illustrate the risk of potential compromise to the organization. The recommendations provided in this report are structured to facilitate remediation of the identified security risks.

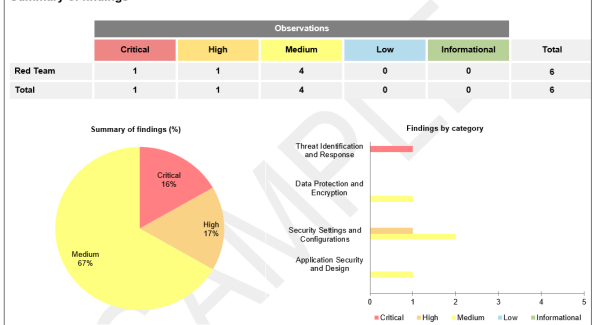
### Scope and Overall Results

EY performed a scenario-based red-team assessment for COMPANY based on organization and industry specific threats. During this efforts, EY assessed COMPANY's information security using a threat based approach that mimics what an actual attacker would use in attempts to access one or several targets or trophies. The techniques used by EY have been designed to emulate the techniques used by the probable threat actors and determined to most likely compromise the agreed-upon targets.

EY and COMPANY agreed upon the following risks, the threat scenarios, as well as the targets and approach for this assessment:

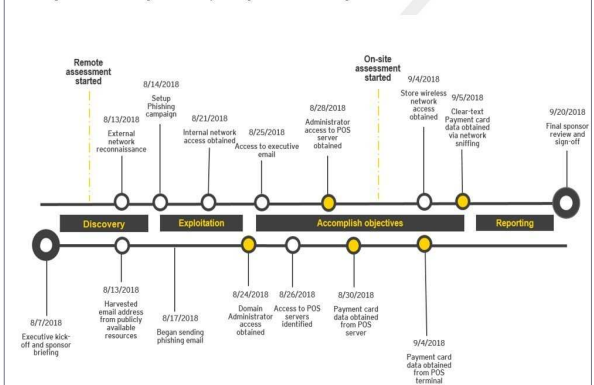
Threat Scenario/Risk	Targets	Approach	Results
1. Exposure of PHI through Internet-facing web applications and systems	<ul style="list-style-type: none"> <li>Member PHI data</li> <li>Member application servers</li> </ul>	<ul style="list-style-type: none"> <li>External network assessment</li> <li>Web application black box assessment</li> </ul>	<ul style="list-style-type: none"> <li>Member PHI data was not obtained</li> </ul>
2. Access to sensitive data (PHI or PCI) by any employee in the COMPANY environment	<ul style="list-style-type: none"> <li>Data Warehouse</li> <li>Back end application database access for sensitive data</li> </ul>	<ul style="list-style-type: none"> <li>Internal network assessment</li> <li>Wireless network scan</li> </ul>	<ul style="list-style-type: none"> <li>Obtained access to Production Data Warehouse</li> <li>Obtained access to application databases</li> </ul>
3. Access to the COMPANY internal network through extranet connected Joint Venture	<ul style="list-style-type: none"> <li>PHI or PCI data</li> <li>Access to data warehouse</li> </ul>	<ul style="list-style-type: none"> <li>Internal network assessment</li> <li>Wireless network scan</li> <li>Network segmentation assessment</li> </ul>	<ul style="list-style-type: none"> <li>Verified access to data warehouse and internal network</li> <li>Obtained access to previously discovered PHI</li> </ul>

### Summary of findings



### Timeline of activities

The following timeline illustrates a high-level summary of the significant milestones throughout the duration of the assessment.



## Executive summary

An executive level presentation to summarize the scope and results of the engagement, a synopsis of the highest risk findings, as well as recommended tactical and strategic next steps.

### Value:

- Executive-level overview of the results
- Prioritized next steps to improve the overall security posture

## Summary of Findings

A summary of findings section consisting of consolidated list of issues and key observation themes as well as positive observations observed during the assessment.

### Value:

- Enables management to understand the big picture of issues identified and summary of strength
- Provides actionable items to address remediation of specific vulnerabilities and control gaps
- Incorporates detection activities and timeline provided by the client upon the conclusion of the test in the executive briefing



# Engagement fees, Assumptions and Team

28 March 2024

Presentation title



# Engagement fees

We approach professional fees with the goal of providing the highest quality service under a fair and equitable arrangement. Our goal is to establish a pricing and service structure that is mutually beneficial and will allow us to devote the quality and quantity of talented professionals that you require and expect. **A detailed report of testing activities is included in each service provided.**

- 
- 
- 
- 

Assessment Options	Fees
External Network Penetration Testing + Social Engineering	\$24,000
Wireless Penetration Testing	\$24,000
Internal Network Penetration Testing	\$46,000
Web Application Penetration Testing	\$23,000
Reporting (Included)	Not Applicable
Findings Presentation (Included)	Not Applicable
Professional Services Total Fees	\$117,000
Estimated Travel Expenses	\$11,000
Estimated Total Fees	\$128,000



- 
- 
- 
-



# Assumptions



## External/Internal penetration testing assumptions



- Penetration tests include automated vulnerability scans and manual techniques.
- External testing on the West Virginia State Lottery’s network will be conducted remotely from EY’s Advanced Security Center.
- Any high-risk issues that arise during testing will be brought to the attention of the project sponsor.
- All testing is not intended to be exhaustive in nature and will utilize a time-boxed approach of 2 week for the external network penetration, 2 weeks for web application penetration testing and 2 weeks for internal testing.
- 8 West Virginia State Lottery locations are in scope for internal testing.
- Internal testing will be conducted at up to 2 locations per day.
- The external and internal penetration testing will include limited stealth testing to evade detection (firewall/IDS) and will utilize time-boxed testing approach.
- West Virginia State Lottery will obtain authorization from third-party providers (if any) prior to the beginning of external penetration testing activities.
- West Virginia State Lottery will provide contact information (email, office and mobile number) for designated technical contact.
- Target list of IP addresses for external, internal network penetration and vulnerability testing will be provided by and confirmed with West Virginia State Lottery’s management.
- West Virginia State Lottery will provide the appropriate access and credentials to be utilized (where needed) for the testing.
- Physical intrusions and will be out of scope of testing.
- 1 phishing scenario will be conducted apart of the external penetration testing.

## Web application penetration testing assumptions

- The tests will be limited to the West Virginia State Lottery application only and any other web applications that are accessible after authenticating to West Virginia State Lottery application will be considered out of scope for testing.
- Testing can be conducted for more than one application at a time and one application may be tested by more than one tester.
- West Virginia State Lottery will provide all in-scope URL’s for testing.
- Penetration tests include automated vulnerability scans and manual techniques.
- No travel is expected for testing activities.



# Assumptions Cont.



## Wireless penetration testing assumptions



- Wireless testing will be conducted in conjunction with the on-site internal penetration testing.
- West Virginia State Lottery will provide access to in-scope facilities.
- 8 West Virginia State Lottery locations are in scope for internal testing.
- West Virginia State Lottery will provide the appropriate access and credentials to be utilized (where needed) for the testing.
- All testing is not intended to be exhaustive in nature and will utilize a time-boxed approach of 2 weeks for the wireless testing.
- Wireless testing will be conducted at up to 2 locations per day.
- Physical intrusions and will be out of scope of testing.



# Team to serve



## Managing Director

### Background

Global Head of Cyber Threat Response, which consists of Incident Response, Threat Hunting, Cyber Readiness and the Insider Threat functions, in a follow-the-sun model with teams in the US, Zurich, Poland, and Singapore.

### Relevant experience

- Oversaw the development and deployment of a new Threat Hunt Platform for data processing and analysis, which streamlined threat hunting data processing and enrichment across the organization and increased efficiency within the team.
- Served as a subject-matter evidence on matters of Cyber Resilience and served as a key stakeholder for building out Cyber Resilience within the firm.
- Served as the Global Head of Cyber Threat Response, in charge of rebuilding the Incident Response function, establishing the Cyber Readiness function, overseeing creation of a new Threat Hunt Platform, implementing the Insider Threat function and playing a key role in building out Cyber Resilience within the firm.
- Established deep relationships with incident response team members where I served as either their Relationship Leader or coach for career growth and training.
- Effectively scoped incident response engagements with appropriate resources based on engagement needs and skill sets

Certifications: Certified Information Systems Security Professional (CISSP), GIAC Certified Forensic Analyst (GCFA), GIAC Certified Forensic Examiner (CCFE), GIAC Certified Incident Handler (GCIH), GIAC Certified Intrusion Analyst (GCIA), GIAC Information Security Professional (GISP) - Active

## Senior Manager

### Background

Pipe is a senior manager in EY's Threat Resiliency Cybersecurity capability, specializing in attack and penetration testing and threat emulation services. With 14 years of diverse information security experience, Pipe has managed and performed hundreds of attack and penetration, attack remediation, and architecture review assessments in various industries, including automotive, hospitality, financial services, insurance, Industrial Control Systems (ICS), Process Control Network (PCN). Pipe presented his cybersecurity thought leadership at leading cyber security conference such as Troopers 2018, BSides Las Vegas 2018, and RSA 2016.

### Relevant experience

- Led the planning and execution for Attack & Penetration Security Assessments for multiple Fortune 500 clients. Manage onshore and offshore delivery resources, provide reporting review and analysis, and conduct executive and technical reporting of strategic and tactical areas of improvement to client stakeholders. Manage a globally distributed team and coordinated resources in the delivery of attack and penetration tests, vulnerability assessments and product security reviews. Oversee the development of various assessment methodologies including external and internal penetration testing, web application security assessments, physical security assessments, wireless assessments and social engineering assessments.
- Assessed 200+ red team assessments for multiple large clients including Fortune 500 organizations. Managed/performed 120+ traditional attack & penetration engagements, including internet, intranet, black box, grey box, segmentation testing and social engineering assessments
- Served as key project manager and technical team lead for a global gaming and hospitality industry leader to perform a security assessment of the corporate internal, guest room, and cruise ship networks. Successfully identified high risk issues and presented the results to key stakeholders including the top tier management executives.
- Certifications: Certified Information Systems Auditor (CISA), GIAC Penetration Tester (GPEN), GIAC Certified Intrusion Analyst (GCIA), GIAC Certified Incident Handler, GIAC Certified Firewall Analyst (GCFW), Oracle Certified Associate (OCA), Hack The Box Pro Lab BlackSky:Cyclone (Cloud Security Specialist)

28 March 2024

West Virginia State Lottery Proposal



# Team to serve Subject Matter Resources

## Penetration Testing Manager

### Background

Penetration Testing Manager has over eight years of experience in information security, network and system administration. His prior roles have equipped him with technical expertise in the realm of penetration testing for both the public and private sectors. Penetration Testing Manager specializes in internal network, external network, web application penetration testing and red team assessments.

Penetration Testing Manager has extensive experience in a consultative role, performing auditing engagements of hardware, software and operational environments. These engagements include compliance, risk, network security and Payment Card Industry (PCI) assessments.

Penetration Testing Manager participates in a number of conferences per year, including Defcon, BSIDES and Shmoocon.

### Relevant experience

- Performed extensive penetration tests on various sectors including clients within the retail, entertainment, healthcare, utility, finance, education sectors and local and federal government.
- Produced advisory reports to developers, engineers and high-level management regarding zero-day exploits, Common Vulnerabilities and Exposures (CVE) vulnerabilities and results from manual testing
- Conducted on-site penetration tests from an insider/outsider threat perspective often traveling domestically to perform high-level penetration tests
- Developed subject matter expertise in focused areas of security

### Certifications

- Offensive Security Certified Professional (OSCP), Red Team Lead (CRTO2), Certified Red Team Expert (CRTE), Certified Red Team Operator (CRTO), Certified Red Team Professional (CRTP), Certified Ethical Hacker (CEH), Security+

## Vulnerability Management Manager

Vulnerability Management Manager in Ernst & Young's Enterprise Vulnerability Management Team. With over 20 years of cyber and IT experience, she is focused on various industries with regards to Vulnerability Management in a variety of areas. These areas include Investigating and troubleshooting all phases of security issues which included, and are not limited to Windows, Unix/Linux systems, vulnerability scanners and related systems to ensure the security of systems and related data.

### Relevant experience

- Managed vulnerability scanning service management. Provided support in activities that involve, performing asset discovery and update/manage scan scope. Configured, schedules, and perform automated vulnerability/compliance scanning on both.
- Delivers technical expertise in a fast-paced growing company related to initiatives in the areas of security operations, development, and deployment, as well as the administrative role in deploying security related systems and cybersecurity.
- Led vulnerability campaigns, providing technical guidance to skillfully integrate the complex Information Management/Information Technology (IM/IT) services required to ensure that the performance of software and equipment is feasible for mission tasking within cyber operations.
- An advisor responsible for ensuring the development and delivery of the strategic vision for Vulnerability Management capabilities working with leadership team.
- Performed Vulnerability Management Audits and Assessments services to provide recommendations to better align the Program with NIST framework, leading practices, reliance, and create overall efficiencies.
- Assisted control owners and client recommendations with their implementation of recently adopted controls and provided clients with process and controls documentation for new control environments (e.g., risk and control matrices, process flowcharts and narratives).

28 March 2024

West Virginia State Lottery Proposal



# Sample Qualifications



## A global hospitality client with sport betting

### EY delivered

- ▶ We performed stealth external and internal attack scenarios at the organization’s headquarter location where we simulated real life attacks targeting critical assets of the organization and then gaining access to sensitive information by utilizing advanced stealth attack techniques.
- ▶ The team was able to leverage server misconfigurations to obtain access to target data as well as the internal network.
- ▶ After gaining access to the internal network, we were successful in gaining access to the following high value targets:
  - ▶ Casino management system
  - ▶ Guest PII

### Outcome obtained

- ▶ Provided a holistic approach to aligning the company’s information security program to current threats and emerging technologies
- ▶ Identified critical security issues within information system and provided actionable remediation strategy

## A large healthcare organization

### EY delivered

- ▶ We performed a stealth scenario-based testing remotely where we executed the following scenarios from the perspective of an assumed breach to an employee computer:
  - ▶ Established a persistent Command-and-Control (C2) channel from the internal network to a consultant-controlled server on the Internet
  - ▶ Simulated a ransomware attack by encrypting files on pre-defined file shares and computers
  - ▶ Exfiltrated a large volume of data from the internal network to an external EY-controlled server
  - ▶ During the fieldwork, we continually observed the organization’s detection and response capabilities to the simulated cyber-attacks

### Outcome obtained

- ▶ Provided insight to the organization’s capabilities for detecting and responding to real-world cyber-attack scenarios such as C2 deployment, ransomware attacks and data exfiltration.
- ▶ Identified critical security issues within information system and provided actionable remediation strategy

## An agriculture product manufacturer

### EY delivered

- ▶ Performed initial compromise of an employee by performing spear phishing attack and then attempted to gain access into the organization’s internal network from the command-and-control (C2)
- ▶ The team also performed physical penetration testing at the organization’s headquarter location to demonstrate circumventing physical controls and gain access to the sensitive information from their internal corporate network
- ▶ After gaining access to the internal network, we attempted to obtain access to a number of targeted systems. This resulted in the following:
  - ▶ Enterprise Administrator level access
  - ▶ Financial data
  - ▶ Executive Email

### Outcome obtained

- ▶ Provided a holistic approach to aligning the company’s information security program to current threats and emerging technologies
- ▶ Leveraged EY’s Cyber Threat Management subject matter resources to augment internal resources and capabilities in implementing the roadmap
- ▶ Identified critical security issues within information system and provided actionable remediation strategy

28 March 2024

West Virginia State Lottery Proposal





# The EY difference — key facts and differentiators

Our knowledge and experiences of A&P across multiple industries enables us to deliver high value and quality services



## Industry

Industry engagement  
Facilitated sessions with industry peers and associations (e.g., FS-ISAC, ISACA, OWASP, etc.).

## Innovation

Innovation sessions  
Research and development session leveraging our industry contacts, help to foster identification of new technologies through relationships with Universities, and bringing thought leadership from our alliance partners (e.g., Microsoft, IBM, and ServiceNow).

## 124 Countries

Our resources have successfully executed cyber assessments in 124 countries, providing a pool of knowledgeable and skilled assessors to leverage globally.

## Access

Transparency  
EY has stringent logical and physical access systems and will allow clients to have transparency into A&P testing facilities and activities.

## Optimization

Monthly optimization reviews  
Meetings for management review on overall statistics, discussing common findings and improvement opportunities, skills and knowledge transfer, and integration with eLearning.

## Commitment to quality

EY is routinely evaluated as a leading service provider when compared to our peers at our current clients.  
Quality Control is embedded in our service delivery process and Quality Assurance acts as the governance quality wrapper around the full model. Quality is not just related to the individual product delivery but also drives challenge and innovation within the model.

## 5000+

Attack and Penetration testing reviews executed across the globe  
EY has successfully executed over 5000 A&P assessments across financial services clients and other industries over the last 21 years, demonstrating our ability to serve the market and ongoing insights to provide better foresight for clients.

## Speed to

Ramping up  
EY has the appropriate mature processes and resources to begin the project once the contract is signed. Additionally, our global capabilities provide regional language support and our existing knowledge of A&P processes allows us to hit the ground running.





# EY's attack and penetration testing capabilities

## Traditional penetration testing

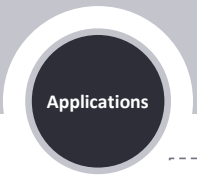
Vector-based approach of specific components — focus on demonstrating extend of risk exposure

## Threat emulation

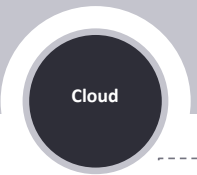
Stealth approach to identify the weakest path to compromise critical business assets — focus on demonstrating resilience against real-world scenarios.



Traditional penetration testing that may include external, internal, and wireless testing. The segmentation between corporate network and other sensitive environments (such as Cardholder Data Environment and Operational Technology) can also be tested.



Test and attempt to exploit the functionality of an application through its interfaces from the perspective of an anonymous user or other authenticated user roles. Typical targets may include web and mobile applications, thick clients, and web services.



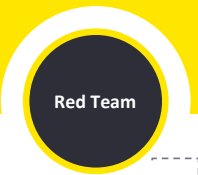
Assess cloud environments for security vulnerabilities that may allow for data leakage or access to unintended environments.



Assess the user security awareness using techniques like physical, phishing, leave-behind media or phone-based attacks that pose a threat to data security.



Assess firmware for security implications and for physical client-side attacks, and experienced resource pool to conduct detailed penetration testing on IoT and connected devices.



Sophisticated attack emulation to deliver adversarial testing that mimics real-world threats targeting your "crown jewels".



We work together with your security team to review the effectiveness of your monitoring and response capabilities as they relate to attack vectors.



Full 4-phased approach to assess, collaborate, and improve your mitigating defensive and responsive countermeasures.



# Biohacking Medical Device CTF win at DEF CON 2019 & 2022



EY's Attack and Penetration Testing team won the DEF CON 30 Biohacking Medical Device Capture the Flag (CTF) competition. The competition took place between August 12-14, 2022 in Las Vegas.



## EY's Advanced Security Center (ASC) certifications

The ASC team stays current by pursuing relevant certifications, participating in and providing internal team training, performing vulnerability research, attending and speaking at security conferences and being involved with a variety of industry groups. The CISSP is required for all ASC team members within their first year. Team members are encouraged to attain other relevant certifications, several of which are listed below:

- Certified Information System Security Professional (CISSP)
- Offensive Security Certified Professional (OSCP)
- Offensive Security Certified Expert (OSCE)
- Offensive Security Web Expert (OSWE)
- Offensive Security Wireless Professional (OSWP)
- GIAC Penetration Tester (GPEN)
- GIAC Web Application Penetration Tester (GWAPT)
- GIAC Mobile Device Security Analyst (GMOB)
- GIAC Exploit Researcher and Penetration Tester (GXPN)
- GIAC Certified Forensic Analyst (GCFA)
- GIAC Defensible Security Architecture (GDSA)
- GIAC Defending Advanced Threats (GDAT)
- GIAC Security Essentials Certification (GSEC)
- Certified Information Security Manager (CISM)
- Cisco Certified Network Associate (CCNA)
- Certified Ethical Hacker (CEH)
- Certified Expert Pen Tester (CEPT)
- Certified Protection Professional (CPP)
- CNSS 4011 Information Security Professional
- GIAC Reverse Engineering Malware (GREM)
- CNSS 4012 Designated Approving Authority
- CNSS 4013 System Administrator
- Certified Information Systems Auditor (CISA)
- CNSS 4014 Information Systems Security Office
- GIAC Certified Firewall Analyst (GCFW)
- Microsoft Certified Technical Specialist (MCTS)
- Oracle Certified Associate (OCA)
- Certified Red Team Professional (CRTP)
- AWS Certified Cloud Practitioner
- AWS Certified Security Specialty
- AWS Certified Solutions Architect
- Associate Azure Security Engineer Associate

## EY | Building a better working world

EY exists to build a better working world, helping create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via [ey.com/privacy](https://ey.com/privacy). EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit [ey.com](https://ey.com).

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

© 2022 Ernst & Young LLP.  
All Rights Reserved.

2207-4075218  
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

[ey.com](https://ey.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  
**Doc Description:** Network Penetration Testing and Cybersecurity Assessments  
**Reason for Modification:**  
**Proc Type:** Central Master Agreement

Date Issued	Solicitation Closes	Solicitation No	Version
2024-03-08	2024-03-28 13:30	CRFQ 0705 LOT2400000009	1

**BID RECEIVING LOCATION**

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

**VENDOR**

**Vendor Customer Code:**  
**Vendor Name :** Ernst & Young LLP  
**Address :** 900 United Center  
**Street :** 500 Virginia Street East  
**City :** Charleston  
**State :** WV **Country :** **Zip :** 25301  
**Principal Contact :** John Leo, Jr.  
**Vendor Contact Phone:** +1 201 551 5007 **Extension:**

**FOR INFORMATION CONTACT THE BUYER**

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

**Vendor Signature X**

**FEIN#** 34-6565596

**DATE** 3/29/2024

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



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**

<b>Proc Folder:</b> 1369290		<b>Reason for Modification:</b>	
<b>Doc Description:</b> 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	
<b>Proc Type:</b> Central Master Agreement			
<b>Date Issued</b>	<b>Solicitation Closes</b>	<b>Solicitation No</b>	<b>Version</b>
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:**  
**Vendor Name :**  
**Address :**  
**Street :**  
**City :**  
**State :** **Country :** **Zip :**  
**Principal Contact :**  
**Vendor Contact Phone:** **Extension:**

**FOR INFORMATION CONTACT THE BUYER**

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

**Vendor Signature X**

**FEIN#** 34-6565596

**DATE** 3/29/2024

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



**ADDENDUM ACKNOWLEDGEMENT FORM**  
**SOLICITATION NO.: LOT2400000009**

**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.

EY \_\_\_\_\_

Company

\_\_\_\_\_  


Authorized Signature

3/28/2024 \_\_\_\_\_

Date

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

Revised 6/8/2012