|  |
| --- |
| Logo of the Centers for Medicare & Medicaid Services, Office of Information Technology.Department of Health & Human Services  Centers for Medicare & Medicaid Services  7500 Security Boulevard, Mail Stop C5-19-16  Baltimore, Maryland 21244-1850    **Office of Information Technology** |
|  |
| Information Security & Privacy Group  **<Insert System Name>** Rules Of Engagementfor Penetration Testing <Insert Date> |
|  |

# Introduction

Under the Federal Information Security Management Act of 2002 (FISMA), the Office of Management and Budget (OMB) directed the National Institute of Standards and Technology (NIST) to develop specific guidance for federal agencies to test and assess the security of their information systems. Network vulnerability assessment and penetration testing of information systems are also procedures recommended in the Security Management and Access Controls portions of the Government Accountability Office (GAO) guidance provided in the Federal Information System Controls Audit Manual (FISCAM). This testing in the CMS enterprise is authorized by CIO Directive 12-01 – *CMS Vulnerability Assessment and Penetration Testing*[[1]](#footnote-1). NIST Special Publication (SP) 800-115, *Technical Guide to Information Security Testing and Assessment*[[2]](#footnote-2), provides specific guidance for conducting these tests and assessments, including guidance for developing Rules of Engagement (ROE). This document follows the National Institute of Standards and Technology (NIST) SP 800-115 ROE format.

This ROE establishes guidelines for Federal staff and Federal Contracting staff to conduct vulnerability assessments and penetration testing of system and network components throughout the CMS Enterprise. Within this document and unless otherwise specified, the terms “test” and “testing” refer to both network vulnerability assessment and penetration testing used to evaluate CMS systems. This document also serves to protect both parties by authorizing Federal staff and Contractor staff’s penetration testing teams to perform vulnerability assessments and penetration tests against CMS assets.

A network vulnerability assessment is a typically automated systematic examination of an information system or product intended to accomplish these objectives:

* Determine whether or not security controls are adequately designed and effectively implemented
* Identify security deficiencies and determine the effectiveness of external perimeter and internal security controls
* Provide a basis for evaluating the effectiveness of proposed or implemented security measures
* Map the vulnerabilities with associated exploits
* Post-implementation confirmation of changes made to the security baseline and other protective measures

Penetration testing is security testing in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application, system, or network. It often involves launching real attacks on real systems and data, using tools and techniques commonly employed by attackers. Most penetration tests involve looking for combinations of vulnerabilities on one or more systems that can be used to gain more access than could be achieved through a single vulnerability. Penetration testing can also be useful for determining:

* How well the system tolerates real-world attack patterns
* The likely level of sophistication an attacker needs to successfully compromise the system
* Additional countermeasures that could mitigate threats against the system
* The defenders’ ability to detect attacks and respond appropriately
* Assess the security posture of the target system
* Identify gaps in the implementation of defense in depth security
* Evaluate device configuration

Once testing is complete, Federal and Contracting staff will work closely with the target system personnel to identify corrective actions needed to remediate vulnerabilities and suggest methods for improvement. Please note that, per section SI-2 of the *CMS Acceptable Risks and Safeguards (ARS) 2.0*[[3]](#footnote-3), System Owners must “Correct identified security-related information system flaws on production equipment within ten (10) business days and all others within thirty (30) calendar days.”

# Scope

CMS ISPG will work with the appropriate stakeholders (application/business owner, ISSO, contractor(s)) to determine the scope of the engagement, and will identify the correct options for testing.

Specific systems and/or networks to be tested, authorized and unauthorized IP addresses, restrictions, exclusions, and/or other guidance will be specified by ISPG in the Penetration Test Schedule found in [Appendix A](#_APPENDIX_A). To promote efficiency, CMS Federal Leads may assist in identifying low-value targets from the list of potential targets identified during network discovery procedures. **CMS Federal Leads have the opportunity, at any time, to identify prohibited systems, times of day, or IP addresses to be excluded from testing.** In general, the following tests will be performed based on whether the testing is external or internal to CMS:

* General:
* Internal and external network and system enumeration
* Internal and external vulnerability scanning
* Information gathering and reconnaissance
* Simulate exfiltration of data
* Simulate or actually download hacking tools from approved external websites
* Attempt to obtain user and/or administrator credentials
* Attempt to subvert operating system security controls
* Attempt to install or alter software on target systems
* Attempt unauthorized access of resources to which the team should not have access
* Application:
* Review the implementation of forms used in browser-based/Web applications and perform input-poisoning attacks
* Review session management controls to ensure that browser-based/Web applications maintain distinct user sessions
* Attempt to subvert applications and database security controls
* Evaluate secure socket layer (SSL) implementation and configuration
* Test susceptibility to SQL injections
* Test susceptibility to other input poisoning

Vulnerability scanning and penetration testing can be performed from the Internet, CMSnet, public areas within CMS facilities, positions gained by internal lateral movement, and/or non-public areas within CMS facilities.

The test team may employ commercial, noncommercial, and custom test and network monitoring tools including, but not limited to the testing tools identified in [Section 4.3](#_Testing_Tools).

# Risks and Limitations

The testing described in this document is sensitive in nature. The testing team will take necessary steps to avoid any adverse impact on CMS Systems from authorized testing. For example, the team will limit any load on the network segments caused by testing and thereby try to avoid a Denial of Service (DoS) for any CMS network resources.

This ROE facilitates testing in a controlled manner that addresses potential and realized impacts on CMS operations while allowing for the most useful test results possible.

The testing team will not target systems outside of the specified IP range(s). However, tools will be sending nonstandard network traffic that could affect non-targeted (out-of-bounds) machines located on the same network. The testing team will make every effort to avoid affecting the availability of targeted IT resources. However, vulnerability assessments and penetration testing are inherently invasive activities.

**The CMS CIO, ISPG, and other components within CMS, including contractors acting on their behalf, will not hold the testing team responsible for any harm to either targeted or non-targeted systems caused by authorized testing activity or any losses caused by interruption of normal operations.**

In an effort to do no harm, the testing team will work closely with system engineers and maintainers to reverse any changes made to systems during the course of testing. Intentional “footprints” left behind as evidence of successful exploits will be addressed after the vulnerabilities/weaknesses are identified, documented and reported.

It is the responsibility of the system owner to confirm that adequate system backups have been performed and that recovery procedures are in place in the unlikely event that a partial or full recovery is needed. System owners are also responsible for documenting their security controls according to NIST Special Publications and CMS policy. Security authorization documentation should include all applicable system information and is not repeated in this document unnecessarily. The CMS CIO and/or CISO (or his/her designate) will coordinate all activities that may affect other government organizations, contractors, network operations centers, and Internet service providers, as appropriate.

CMS Penetration Testing Team personnel may, but are not required to be, onsite during the testing. In the event that a recovery is needed, the Federal and\ or contracting staff will contact appropriate target environment personnel listed in the [Key Personnel](#_Key_Personnel) section of this document.

# Logistics

## Key Personnel

Many CMS systems and programs process sensitive information. Test team members will be cleared to work on the project by the Department of Health and Human Services (HHS) and/or CMS. Consistent with the sensitivity of the information, the testing team is responsible for protecting interim results, work papers, and summaries of results from unauthorized disclosure.

To support testing integrity, all parties having knowledge of the testing activity are requested to restrict communication to the operational level on matters such as, but not limited to, testing schedules, the types of tests to be performed, the results sought, and other information as described herein.

| Organization | POC Name | Role/Responsibility | Phone Number/ Email Address |
| --- | --- | --- | --- |
| CMS/OEI/ISPG | Paul Newton | Penetration Testing Program Manager | 410-786-0749  [Paul.newton1@cms.hhs.gov](mailto:Paul.newton1@cms.hhs.gov) |
| CMS/OEI/ISPG Contractor | Jonathan Wohlberg | Penetration Testing Team Lead | Jonathan.wohlberg@cms.hhs.gov |
| CMS/OEI/ISPG Contractor | Brian Conte | Senior Penetration Tester | 410-786-0151  [Michael.Conte@cms.hhs.gov](mailto:Michael.Conte@cms.hhs.gov) |
| CMS/OEI/ISPG Contractor | Adam Willard | Senior Penetration Tester | 410-218-7352  [Adam.Willard@cms.hhs.gov](mailto:Adam.Willard@cms.hhs.gov) |

CMS ISPG may assign a monitor to assist in and review the testing process during the testing period of performance. Personnel changes will be reflected in the Penetration Test Plan, as appropriate.

## Test Schedule

A briefing will be given to applicable data center/system POCs (e.g., Business Owner, Information System Security Officers, etc.) describing the overall methodology for the specific testing that will be conducted. This testing methodology will be detailed in the Penetration Test Plan, based upon the scope and magnitude of the specific test. The Test Plan will be updated as necessary based upon the discussions conducted at the Test Methodology Briefing.

Target environment personnel will provide the following information to CMS ISPG a minimum of **5 business days** prior to the initiation of testing (note that the 5 business day requirement may be waived depending on certain tests):

* Period of testing performance – Specific times for all testing will be contained in individual Test Plans. However, most testing will be conducted between the hours of 8:00 A.M. and 6:00 P.M. U.S. Eastern Time, Monday through Friday unless otherwise stated within the individual Test Plans.
* Target environment resources to be tested (IP addresses, Hostname, URL)
* Any restricted hosts, systems, or subnets that are not to be tested

CMS ISPG will work with appropriate target environment personnel to identify the following information prior to the commencement of testing:

* Depending on the type of test performed (Announced / Unannounced), IP addresses from which testers will conduct vulnerability assessments and penetration testing

Testing status updates and any key findings will be discussed daily with target system personnel. Meeting minutes will be provided within 48 hours after the daily meeting. Testing activities will be documented in a manner that will enable the tests to be repeatable, by appropriate and qualified parties.

| Milestone | Planned Date |
| --- | --- |
| Overall Testing Methodology Briefing | As specified in the Penetration Test Plan |
| ISPG restrictions/guidance due to testing team | As specified in the Penetration Test Plan |
| Updated Testing Plan (due 5 days prior to test) | As specified in the Penetration Test Plan |
| Testing Dates | As specified in the Penetration Test Plan |
| Draft Test Results to be Presented to ISPG | As specified in the Penetration Test Plan |
| Draft Test Results to be Presented to Data Center Management | As specified in the Penetration Test Plan |
| Final Test Report and Corrective Action Plan Worksheet | As specified in the Penetration Test Plan |

Federal and Contracting Personnel will coordinate the completion of the Penetration Test Plan, agreements, and scheduling to facilitate the execution of testing. This includes the completion of these Rules of Engagement, the Penetration Test Plan, setting up the overall testing methodology briefing, initiating daily status briefings during the testing, and scheduling the report reviews at the conclusion of testing.

## Testing Tools

Vulnerability assessment and penetration testing tools include commercial, non-commercial, custom built, as well as network monitoring tools that have been pre-approved for use by CMS. A general list of the current CMS Vulnerability Assessment and Penetration Testing Tool Suite is provided below. In the event that additional tools are identified as necessary for a specific vulnerability assessment or penetration test, these tools will be documented within the Penetration Test Plan, and approved for use by ISPG prior to the use of said tool.

Tools included in the CMS Vulnerability Assessment and Penetration Testing Tool Suite:

| Testing Tools | |
| --- | --- |
| Achilles | Nmap |
| AppScan | Openssl |
| Cookie Digger | Oracle Auditing Tools (OAT) |
| Core Impact | Oracrack |
| Curl | Paros |
| DNSstuff | Rapid7 NeXpose |
| Google | SiteDigger |
| Httprint | SpikeProxy |
| Httrack | SSLDigger |
| John the Ripper | Stunnel |
| Kali Linux | THC-Hydra |
| MetaCoretex | Wayback Machine |
| Metasploit Pro | WebInspect |
| Ncat | WebScarab |
| Nessus w/ professional feed | Wget |
| Netcraft | Wireshark |
| Nikto |  |

# Incident Handling and Response

This document, when signed by appropriate personnel, will serve as formal permission granted by CMS, and target system personnel, for the CMS Penetration Testing team to undertake the testing described herein. **Should CMS or target system personnel detect and formally report testing activities to law enforcement, this document will be used to advise law enforcement officials of authorized testing activities.**

If the testing process identifies a significant weakness or vulnerability, the vulnerability will be brought to the immediate attention of the appropriate entities to facilitate corrective action.

If the testing team identifies suspicious artifacts or activity during testing, and suspects that they have encountered an incident in progress or evidence of an incident having already taken place, they will immediately cease testing and report the suspected incident to the CMS IT Service Desk, target system personnel, and appropriate CMS Points of Contact, in accordance with the *CMS Incident Handling and Breach Analysis/Notification Procedures*[[4]](#footnote-4)*.*

# Termination of Testing

If the Penetration testing team is not able to gain access to target environment systems in accordance with the budgeted level of effort, the testing will cease. If the Penetration Testing Team is able to gain access, revealing the capability for exploitation, the vulnerability shall be documented according to CMS guidance. In addition, testing will terminate if the Penetration Testing Team, in consultation with CMS ISPG, determines that any of the following conditions exist:

* Unexpected occurrences are encountered that prohibit further testing
* The CMS Federal Lead reports that testing procedures materially affect computer operations in a negative manner

In the event that the testing team is able to exploit a vulnerability or weakness that allows them to elevate access and/or privileges that affords the testing team’s ability to take control of the organizations’ networks or user administration tools; details of the vulnerability / exploit will be reported to key stakeholders on a “need to know” basis.

After testing has been completed, the testing team will make all reasonable efforts to remove test software from target networks, servers, workstations and devices and will work with IT system engineers to undo any configuration changes to systems.

Should the need for an interruption of testing arise, a communication should be sent to all individuals identified in the Key Personnel section.

If CMS ISPG or target system personnel desires to resume testing that has been interrupted, the following steps will be taken.

* If less than 48 hours have elapsed since the test was interrupted AND the testing personnel and resources are still available, notification of Federal staff and/or Federal Contracting staff listed in Key Personnel section is required.
* Should a scheduling conflict exits, the test will be rescheduled for a later date. The Penetration Test Schedule documents will be updated to reflect specific details, as appropriate.

# Data Handling

All associated with the test in any way are responsible for protecting interim results, work papers, and summaries of results from unauthorized disclosure consistent with the sensitivity of the information.

All sensitive data, at rest or in transit, must be encrypted. All deliverables will be protected and marked as sensitive.

Upon completion of testing and delivery of all final reports, any data collected during test shall be destroyed unless otherwise agreed upon in writing. Receipts for destruction will be provided to CMS.

Any special handling instructions for a specific assessment will be documented within the Penetration Test Plan.

# Reporting

The testing team will coordinate with, and report to a CMS ISPG representative during test activities.

Federal and Contracting staff shall brief target system personnel on the results of testing and provide copies of supporting documents.

Upon completing the activities identified in the test plan, the testing team will prepare a test report identifying the actions taken as well as the results of the test. This report will be provided to target environment Federal and contracting personnel as appropriate. These test reports will provide both a narrative and the technical details of the test, to include:

* Executive Summary – A summary of all findings
* Attack Narrative/Timeline – Details on the exploitation tactics used
* Vulnerability details – Details on each vulnerability found, ranked based upon likelihood and impact. The following information is provided for each vulnerability:
* Risk rating (i.e. High, Medium, Low)
* Affected system (i.e. webserver XXXX, database XXXX)
* Impact (i.e. By utilizing public exploit “X,” root level privileges can be obtained)
* Public exploit (i.e. https://www.exploit1234.com) (if applicable)
* Remediation (i.e. Apply vendor-supplied patched to update file “X” to a greater version.
* List of changes made (if applicable)
* Remediation/mitigation recommendations (if applicable)
* Appendices containing supporting documentation (as required)

# Warranty, Limitation of Liability, and Indemnification

Security vulnerability assessment and penetration testing activities are designed to be non-destructive. The CMS Penetration Testing Team adheres to a “do no harm” approach. However, some tests may have a noticeable effect on performance, cause heavy network traffic, disrupt normal network activity, or cause the target resource to halt. Federal staff and/or Federal Contracting staff warrants that vulnerability assessment and penetration testing will not intentionally disrupt or damage the systems tested.

**The CMS CIO and CISO (or other Designated Approving Authority) agrees to come to the aid of Federal staff and/or Federal Contracting staff** **and the testing team members listed in this Rules of Engagement document and associated test plans if law enforcement should detain them in any manner.**

**IN NO EVENT SHALL Federal staff and/or Federal Contracting staff** **BE LIABLE FOR:**

**(a) Any special incidental, consequential, direct or indirect damages (including, without limitation, damages for loss of profits, business interruption, loss of programs or information, and the like) arising out of authorized testing, even if Federal staff and/or Federal Contracting staff** **or any of its authorized representatives or subcontractors has been advised of the possibility of such damages,**

**(b) Any claim attributable to errors, omissions, or other inaccuracies in the testing, or**

**(c) Any claim by any third party.**

**Because some states do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitations may not apply to approving authority or customer. In the event that applicable law does not allow the complete exclusion or limitation of liability of claims and damages as set forth in this agreement, Federal staff and/or Federal Contracting staff’s** **liability is limited to the greatest extent permitted by law.**

**(For Federal Contractors Only) Approving authority and customer hereby indemnifies, defends, and holds harmless The Federal and Contractor staff, its board of trustees, officers, agents, employees and subcontractors from any and all liability for damages to approving authority, customer, or any third party which may arise, including but not limited to claims for violation of privacy laws. Such indemnification shall include any and all damages, including attorneys’ fees and any other related costs and expenses.**

# Signatures

The following parties have acknowledged and agree to the objectives, scope, rules and notification procedures described in this document. Signature below constitutes authorization for Federal staff and/or Federal Contracting staff to commence with the vulnerability assessment and penetration testing described above. All signatures are required.

|  |  |
| --- | --- |
| [target environment personnel]  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  NAME  POSITION / GROUP | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Date |
| [CMS Business Owner]  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  NAME  POSITION / GROUP | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Date |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Penetration Testing Program Manager  Information Security & Privacy Group | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Date |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Kevin Allen Dorsey  CMS Deputy Chief Information Security Officer | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Date |

# APPENDIX A: Penetration Test Plan

**Internal IP Addresses tested from CMS BDC**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

External IP addressed tested from: ##.###.###.## and ###.##.##.##

|  |  |
| --- | --- |
|  |  |

1. CIO Directive 12-01 – CMS Vulnerability Assessment and Penetration Testing (<http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/CIO-Directives-and-Policies/CIO-Directives-List-Items/CIODirective1201.html?DLPage=1&DLEntries=10&DLSort=2&DLSortDir=descending>) [↑](#footnote-ref-1)
2. NIST Special Publication (SP) 800-115, Technical Guide to Information Security Testing and Assessment (<http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf>) [↑](#footnote-ref-2)
3. CMS Acceptable Risks and Safeguards (ARS) 2.0 (<http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html>) [↑](#footnote-ref-3)
4. CMS Incident Handling and Breach Analysis/Notification Procedures. [(http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/RMH-Vol-II-Procedure-7-2-%C2%A0Incident-Handling-Procedure.html).](file:///C:/Users/N35Q/AppData/Local/Microsoft/Windows/Temporary%20Internet%20Files/Content.Outlook/DJYJA5FD/(http:/www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/RMH-Vol-II-Procedure-) [↑](#footnote-ref-4)