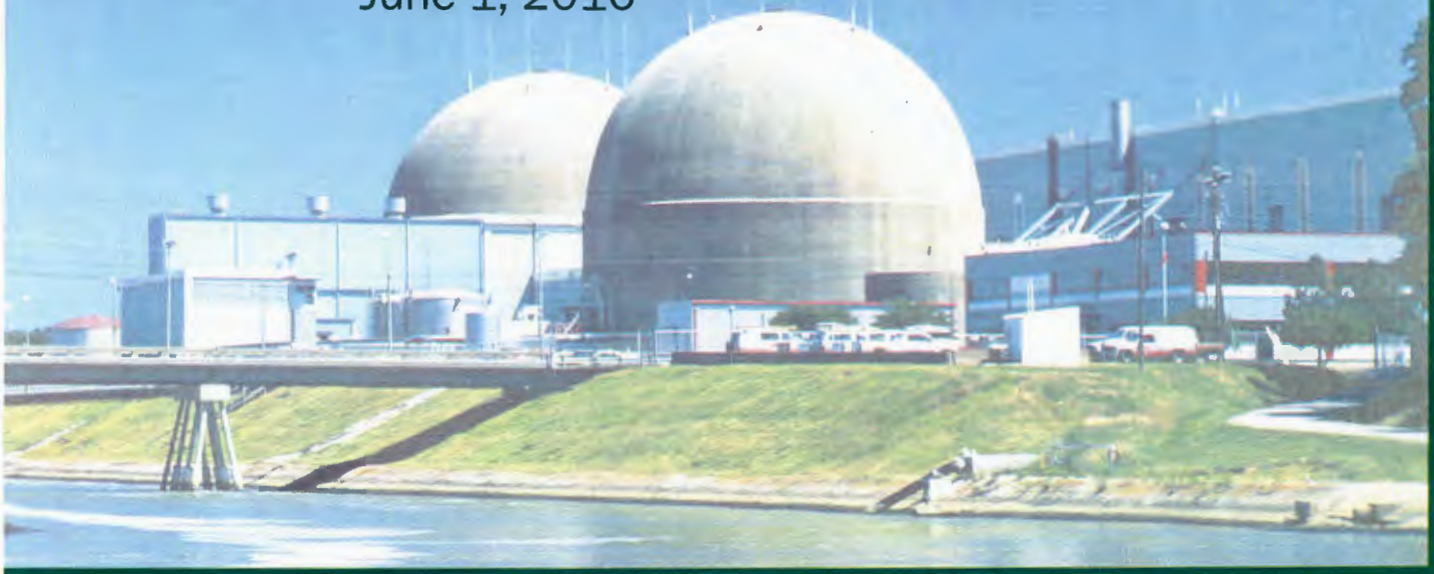
OFFICE OF THE INSPECTOR GENERAL

U.S. NUCLEAR REGULATORY COMMISSION
DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Independent Evaluation of the Security of NRC's Publicly Accessible Web Applications

OIG-16-A-15
June 1, 2016



All publicly available OIG reports (including this report) are accessible through NRC's Web site at
http://www.nrc.gov/reading-rm/doc-collections/insp-gen

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

OFFICE OF THE
INSPECTOR GENERAL

June 1, 2016

MEMORANDUM TO: Victor M. McCree
Executive Director for Operations

FROM: Stephen D. Dingbaum
Assistant Inspector General for Audits

SUBJECT: INDEPENDENT EVALUATION OF THE SECURITY OF NRC'S PUBLICLY ACCESSIBLE WEB APPLICATIONS (OIG-16-A-15)

Attached is the Office of the Inspector General's (OIG) report titled *Independent Evaluation of the Security of NRC's Publicly Accessible Web Applications.*

The report presents the results of the subject evaluation. Following the May 18, 2016, exit conference, agency staff indicated that they had no formal comments for inclusion in this report.

Please provide information on actions taken or planned on each of the recommendations within 30 days of the date of this memorandum. Actions taken or planned are subject to OIG followup as stated in Management Directive 6.1.

We appreciate the cooperation extended to us by members of your staff during the evaluation. If you have any questions or comments about our report, please contact me at (301) 415-5915 or Beth Serepca, Team Leader, at (301) 415-5911.

Attachment: As stated

Office of the Inspector General

U.S. Nuclear Regulatory Commission
Defense Nuclear Facilities Safety Board

OIG-16-A-15

June 1, 2016

Results in Brief*

Why We Did This Review

The U.S. Nuclear Regulatory Commission (NRC) manages numerous publicly accessible Web applications to share nuclear information with licensees and the public. NRC publicly accessible Web applications consist mainly of Web sites, but also include Web-based login portals and administrative systems that provide authorized personnel remote access to agency information technology (IT) resources. NRC is a regular target of cyber-attacks because its technical and other sensitive information is highly sought after by potential adversaries.

The NRC Office of Inspector General (OIG) has joined other OIGs to conduct a Federal-wide review of publicly accessible Web applications and associated security controls. Each OIG will assess its own agency's Web applications program, allowing the OIG group to then develop Federal-wide recommendations and best practices to secure and manage publicly accessible Web applications.

The objective was to determine (i) the effectiveness of NRC's efforts to secure its publicly accessible Web applications, and (ii) whether NRC has implemented adequate security measures to reduce the risk of compromise for their publicly accessible Web applications.

Independent Evaluation of the Security of NRC's Publicly Accessible Web Applications

What We Found

NRC has developed several policies, procedures, processes, and standards for ensuring NRC systems and applications are implemented in a secure manner, including guidance specific to the development of Web applications. However, the evaluation team found that NRC's efforts to secure its publicly accessible Web applications may not be effective and NRC has not implemented adequate security measures to reduce the risk of compromise for their publicly accessible Web applications. Specifically, the evaluation identified the following weaknesses:

- NRC does not have an inventory of publicly accessible Web applications.
- NRC cyber security standards are not current.
- NRC Web applications may not be compliant with NRC cyber security standards.
- Authorization to operate the NRC Webcast Portal did not follow the NRC Risk Management Framework process.
- NRC's IT system decommissioning process needs improvement.

What We Recommend

To improve the security of NRC's publicly accessible Web applications, we make recommendations. Management stated their general agreement with the findings and recommendations in this report.

*This is an OIG-prepared Results in Brief that summarizes the results and activities of the contractor's independent evaluation.

TABLE OF CONTENTS

ABBREVIATIONS AND ACRONYMS

CIGIE	Council of the Inspectors General on Integrity and Efficiency
DHS	Department of Homeland Security
DNS	Domain Name Service
FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Management Act
FISMA 2014	Federal Information Security Modernization Act of 2014
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
ISD	Information Security Directorate
IT	Information Technology
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
OCIO	Office of the Chief Information Officer
OIG	Office of the Inspector General
OMB	Office of Management and Budget
OWASP	Open Web Application Security Project
RMF	Risk Management Framework
SP	Special Publication
SSL	Secure Sockets Layer
SWG	Standards Working Group
TLS	Transport Layer Security

I. BACKGROUND

The U.S. Nuclear Regulatory Commission (NRC) manages numerous publicly accessible[1] Web applications to share nuclear information with licensees and the public. NRC publicly accessible Web applications consist mainly of Web sites, but also include Web-based login portals and administrative systems that provide authorized personnel remote access to agency information technology (IT) resources. NRC is a regular target of cyber-attacks because its technical and other sensitive information is highly sought after by potential adversaries.

As part of a Council of the Inspectors General on Integrity and Efficiency (CIGIE) IT Subcommittee crosscutting project, NRC Office of Inspector General (OIG) has joined 15 other OIGs to conduct a Federal-wide review of publicly accessible Web applications and associated security controls. Each OIG will assess its own agency's Web applications program, allowing the OIG group to then develop Federal-wide recommendations and best practices to secure and manage publicly accessible Web applications.

NRC OIG retained Richard S. Carson & Associates, Inc. (Carson Inc.) to assess NRC's publicly accessible Web applications as part of this crosscutting project. The evaluation was performed with the full cooperation of NRC. NRC perimeter security services (e.g., firewalls, intrusion detection/prevention systems) were configured to whitelist (i.e., monitor only, not block) the scanning platforms/hosts identified in the agreed upon rules of engagement. The evaluation team did not make any attempts to test the effectiveness of such perimeter security services. This report presents the results of the evaluation.

[1] For the purposes of this evaluation, the term "publicly accessible" is defined as "Online resources and services available over HTTP or HTTPS over the public Internet that are maintained in whole or in part by the Federal Government and operated by an agency, contractor, or other organization on behalf of the agency. They present government information or provide services to the public or a specific group and support the performance of an agency's mission. This definition includes all Web interactions, whether a visitor is logged-in or anonymous." [Source: Office of Management and Budget (OMB) Memorandum M-15-13, *Policy to Require Secure Connections Across Federal Websites and Web Services*, June 8, 2015]

II. OBJECTIVE

The objective was to determine (i) the effectiveness of NRC's efforts to secure its publicly accessible Web applications and (ii) whether NRC has implemented adequate security measures to reduce the risk of compromise for their publicly accessible Web applications. The Appendix contains a description of the evaluation objective, scope, and methodology.

III. FINDINGS

NRC has developed several policies, procedures, processes, and standards for ensuring NRC systems and applications are implemented in a secure manner. These include:

- Management Directive and Handbook 12.5, *NRC Cyber Security Program.*
- NRC Cyber Security Standards.
- Information Security Directorate (ISD) procedures, processes, guidance, and checklists.
- CSO-PROS-2030, *NRC Risk Management Framework (RMF) and Authorization Process.*

Specific to the development of Web applications NRC has issued the following guidance:

- Management Directive and Handbook 3.14, *U.S. Nuclear Regulatory Commission Public Web Site.*
- CSO-STD-1108, *Web Application Standard.*
- CSO-STD-1314, *NRC Web 2.0 Implementation Standard.*

- CSO-PROS-1314, *NRC Web 2.0 Implementation Authorization Process.*

- Publishing guidance (an NRC Web site) for external Web pages.

However, the evaluation team found that NRC's efforts to secure its publicly accessible Web applications may not be effective and NRC has not implemented adequate security measures to reduce the risk of compromise for their publicly accessible Web applications. Specifically, the evaluation identified the following weaknesses:

- NRC does not have an inventory of publicly accessible Web applications.

- NRC cyber security standards are not current.

- NRC Web applications may not be compliant with NRC cyber security standards.

- Authorization to operate the NRC Webcast Portal did not follow the NRC RMF process.

- NRC's IT system decommissioning process needs improvement.

A. NRC Does Not Have an Inventory of Publicly Accessible Web Applications

While there is no specific requirement to maintain an inventory of publicly accessible Web applications, two current IT security mandates, with which all Federal agencies are required to comply, indicate the need for such an inventory. NRC could not provide a comprehensive inventory, requiring the evaluation team to use several sources of information to identify potential targets for the assessment. The NRC Office of the Chief Information Officer (OCIO) is responsible for maintaining a current and authoritative IT system and asset inventory; however, this inventory pertains to physical assets. System owners are not required to identify whether any of the assets belonging to their system includes publicly accessible Web applications. NRC is often the target of cyber-attacks while at the same time is obligated to be more accessible and transparent to the public. In order to implement adequate security measures to reduce

the risk of compromise, NRC must first identify the potential targets of such attacks.

What Is Required

While there is no specific requirement to maintain an inventory of publicly accessible Web applications, two current IT security mandates with which all Federal agencies are required to comply indicate the need for such an inventory.

Department of Homeland Security (DHS) Cyber Hygiene Assessments

In January 2012, DHS initiated the Cyber Hygiene initiative to assess, on a recurring basis, the "health" of unclassified Federal civilian hosts reachable via the Internet. Cyber Hygiene activities consist of network mapping, vulnerability scanning, and configuration review of common services (e.g. Domain Name Service (DNS)) for errors or deviations from accepted best practice.

Agencies provide the DHS National Cybersecurity Assessment and Technical Services with a list of hosts to scan and scans are performed on a weekly basis. The results from the Cyber Hygiene assessments provide NRC with data and analysis to assist in reducing cybersecurity risk and in identifying and reporting on vulnerabilities and configuration issues present on those hosts before those vulnerabilities can be exploited by a malicious third party.

The success of this type of assessment is highly dependent on providing DHS with a complete inventory of publicly accessible cyber assets, networks, and systems.

Office of Management and Budget (OMB) Memorandum M-15-13, *Policy to Require Secure Connections across Federal Websites and Web Services*

OMB memorandum M-15-13, dated June 8, 2015, requires all publicly accessible Federal Web sites and Web services to provide services through a secure connection (i.e., hypertext transfer protocol secure (HTTPS)). The memorandum requires Federal agencies to deploy

HTTPS on their domains by making all existing Web sites and services accessible through a secure connection by December 31, 2016. As with the DHS Cyber Hygiene assessments, compliance with the requirements in the OMB memorandum requires a complete inventory of all publicly accessible Web sites and Web services.

What We Found

NRC Could Not Provide a Comprehensive Inventory of Publicly Accessible Web Applications

NRC provided an initial list of potential target internet protocol (IP) addresses in response to the evaluation team's initial documentation request. Potential target IP addresses were also identified from the following documentation provided by NRC:

- IP addresses (targets) from a recent penetration testing engagement.
- IP addresses from the NRC DNS servers (DNS dump).
- DHS Cyber Hygiene scan reports.

Additional potential targets were identified from review of system security plans for all NRC systems and from port scans of IP ranges provided by NRC. However, none of the requested documentation provided a comprehensive inventory of publicly accessible Web applications.

The evaluation team identified 106 potential targets (unique hosts or Web sites) from all of the above-mentioned sources. The following are some characteristics of the target population.

- 15 targets were not provided by NRC.
- 65 targets were included in the list of IP addresses from a recent penetration testing engagement.
- 86 targets were found in the NRC DNS dumps.

- 77 targets were included in recent DHS Cyber Hygiene scans.

It should be noted that prior to January 11, 2016, the target list for the DHS Cyber Hygiene scans only included 12 IP addresses.

Why This Occurred

NRC Cyber Security Program Does Not Require an Inventory of Publicly Accessible Web Applications

Management Directive and Handbook 12.5 states OCIO is responsible for maintaining a current and authoritative IT system and asset inventory that identifies all hardware and software that belongs to a specific system. However, this inventory pertains to physical assets. System owners are not required to identify whether any of the assets belonging to their system includes publicly accessible Web applications.

Why This Is Important

Security Measures May Not Be Adequate to Reduce Risk of Compromise

Federal departments and agencies develop and maintain thousands of publicly accessible Web applications to share information, collaborate, and conduct business with the public and business partners, as well as to provide agency and contractor employees with remote access capabilities to internal networks. NRC is often the target of cyber-attacks while at the same time is obligated to be more accessible and transparent to the public. In order to implement adequate security measures to reduce the risk of compromise, NRC must first identify the potential targets of such attacks.

Recommendations

OIG recommends that the Executive Director for Operations

1. Develop and document procedures for ensuring publicly accessible Web applications are assigned a system owner with responsibility for ensuring adequate security measures are in place for those applications.

2. Develop and document procedures for ensuring publicly accessible Web applications are incorporated into an approved system authorization boundary and for clearly identifying those applications in system authorization documentation.

3. Develop and document procedures for ensuring DHS is notified of any changes to the population of publicly accessible Web applications to be included in Cyber Hygiene scans.

B. NRC Cyber Security Standards Are Not Current

Federal guidance requires organizations to review and update policies and procedures at an organization-defined frequency. NRC cyber security standards and processes define this frequency to be at least annually and when any of several conditions exist, such as a change to the threat environment or a vulnerability is discovered that poses a significant risk to NRC and for which a revision to a cyber security standard can mitigate that risk. The evaluation team reviewed several NRC cyber security standards to gain an understanding of NRC security requirements applicable to ensuring Web applications are secure; however, none of them was current and some had not been updated in over 6 years. The NRC process for maintaining standards was not followed as evidenced by changes in the threat environment that should have dictated an update to the standards. NRC cyber security standards are intended to ensure that IT systems are configured to minimize unauthorized access, use, disclosure, change, deletion, or loss of availability of NRC information. However, if the standards are not updated when there are changes to the threat environment, NRC may fail to implement adequate security measures to reduce the risk of compromise introduced by new threats and vulnerabilities.

What Is Required

Federal Guidance Regarding Standards Maintenance

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, provides a catalog of security and privacy controls for federal information systems and organizations. Controls are organized into 18 families. Each family contains security controls related to the general security topic of the family. The first control in each family addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in that family. Policies and procedures should be reviewed and updated at an organization-defined frequency.

Internal Guidance Regarding Standards Maintenance

NRC-Defined Values for System Security and Privacy Controls

CSO-STD-0020, *Organization-Defined Values for System Security and Privacy Controls*, defines the required NRC values for specific computer security and privacy controls identified in Federal computer control standards and guidance. The standard states policies and procedures shall be reviewed at least annually and updated as needed.

NRC Process for Standards Maintenance

CSO-PROS-3000, *Process for Development, Establishment, and Maintenance of NRC Cyber Security Standards*, provides the process used by the ISD and the Standards Working Group (SWG) to develop, establish, and maintain cyber security standards for information systems that store, transmit, receive, or process NRC information. NRC cyber security standards (i) ensure that IT systems are configured to minimize unauthorized access, use, disclosure, change, deletion, or loss of availability of NRC information, (ii) are the source of enterprise-wide cyber security requirements and baseline system configurations within the agency, and (iii) are mandatory.

The ISD and the SWG review all NRC cyber security standards on an annual basis (at a minimum) for routine changes or updates. For example, standards should be reviewed when there is a change to the threat environment or a vulnerability is discovered that poses a significant risk to NRC and for which a revision to a cyber security standard can mitigate that risk.

What We Found

NRC Cyber Security Standards Are Not Current

The evaluation team reviewed several NRC cyber security standards to gain an understanding of NRC security requirements applicable to ensuring Web applications are secure, including, but not limited to, the following:

- CSO-STD-1108, *Web Application Standard*, v1.0, December 1, 2012.
- CSO-STD-4000, *Network Infrastructure Standard*, v1.1, July 18, 2014.
- CSO-STD-2008, *Network Protocol Standard*, v1.0, December 1, 2010.
- CSO-STD-2009, *Cryptographic Control Standard*, V1.0, March 2, 2010.

None of these standards is current, and two have not been updated in over 6 years.

Why This Occurred

Internal Process for Maintaining Standards Was Not Followed

CSO-PROS-3000 requires the ISD and the SWG to review all NRC cyber security standards on an annual basis (at a minimum), including when

there is a change to the threat environment or a vulnerability is discovered that poses a significant risk to NRC and for which a revision to a cyber security standard can mitigate that risk. However, there is no evidence that this review and update occurred as required.

For example, the following are some examples of NRC cyber security standards that should have been updated due to changes to the threat environment:

- CSO-STD-1108, *Web Application Standard* – references the 2007 and 2010 Open Web Application Security Project (OWASP) Top Ten List.[2] The current OWASP Top 10 was released in June 2013.

- CSO-STD-2008, *Network Protocol Standard* – allows SSL V3.0 and TLS V1.0 for implementing secure connections (i.e., HTTPS).[3] These protocols are no longer considered strong cryptography per NIST SP 800-52 Revision 1, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*, which was published April 2014.

- CSO-STD-2009, *Cryptographic Control Standard* – references the use of depreciated hash algorithms and minimum key lengths, which should no longer be used per NIST SP 800-57 Revision 4, *Recommendation for Key Management, Part 1: General*, which was published January 2016 (Revision 3 was published July 2012).

Why This Is Important

Security Measures May Not Be Adequate to Protect Against New Threats

NRC cyber security standards are intended to ensure that IT systems are configured to minimize unauthorized access, use, disclosure, change, deletion, or loss of availability of NRC information. However, if the

[2] https://www.owasp.org/index.php/Top_10_2013-Top_10 The Open Web Application Security Project (OWASP) is a worldwide not-for-profit organization providing free materials regarding software security risks. The OWASP Top Ten is an awareness document that represents a broad consensus about the most critical web application security flaws.

[3] SSL – secure sockets layer, TLS – transport layer security.

standards are not updated when there are changes to the threat environment, NRC may fail to implement adequate security measures to reduce the risk of compromise introduced by new threats and vulnerabilities. For example, testing found 12 targets that support TLS V1.0.

Recommendation

OIG recommends that the Executive Director for Operations

4. Develop a plan and schedule to identify, review, and update all NRC cyber security standards that have not been updated in the past 12 months.

C. NRC Web Applications May Not Be Compliant With NRC Cyber Security Standards

NRC has developed cyber security standards for protecting Web applications from vulnerabilities and for meeting all federally mandated and NRC-required security requirements. Of the 106 potential targets (unique hosts or Web sites) identified during testing, 38 had Web applications that could be tested, and each one had at least one vulnerability that fell within the OWASP Top 10 Web application security flaws or weaknesses. An important cause of these weaknesses is confusion regarding which NRC office is responsible for ensuring adequate security measures are in place for contractor-operated systems, especially Web applications. The configuration of an information system and its components has a direct impact on the security posture of the system. If configuration management and patch management procedures are not consistently implemented, information security protections may not be commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of NRC information and information systems.

What Is Required

NRC Web Application Standards

CSO-STD-1108 provides descriptions and protection methods for major Web application vulnerabilities that must not be present for Web applications in the NRC production environment. All NRC Web applications in production within NRC must be protected against the vulnerabilities identified in this standard and must meet all federally mandated and NRC-required security requirements. The standard includes but is not restricted to Web applications that are commercial off-the-shelf software, government off-the-shelf software, custom developed applications, and/or any combination thereof. While CSO-STD-1108 has not been updated to explicitly list the current OWASP Top 10, it does state that ISD is tasked with performing Web application assessments against the most recent OWASP Top 10 List. Any deviations from the standard must be documented and approved in accordance with the agency's deviation process as outlined in CSO-PROS-1324, *US NRC Deviation Request Process*.

What We Found

Possible Noncompliance With Web Application Standards

The evaluation team developed an inventory of potential targets from information provided by NRC, as well as from review of system security plans for all NRC systems, and from port scans of IP ranges provided by NRC. The evaluation team then tested publicly accessible Web applications using industry standard Web application scanning tools.

Of the 106 potential targets (unique hosts or Web sites) identified during testing, 38 had Web applications that could be tested. In order to be tested, a Web application needed to reply with one or more interactive pages when queried on one of the commonly used Web application ports (e.g., ports 80 and 443).

Each of the Web applications tested had at least one vulnerability that fell within the OWASP Top 10 Web application security flaws or weaknesses. The most common vulnerabilities were A5 – Security Misconfiguration and A6 – Sensitive Data Exposure. One host was affected by five of the OWASP Top 10. The evaluation team's analysis did not include determining if there were any existing compensating controls or approved deviations for these vulnerabilities.

During fieldwork, NRC was immediately notified of two vulnerabilities with a potential high impact. The first was a router with an Internet-accessible Web administration interface. The other was a cross-site scripting vulnerability on a PKI Services page. Both vulnerabilities were remediated within 24 hours of notification to NRC. The evaluation team confirmed the vulnerabilities were remediated.

Why This Occurred

An important cause of these weaknesses is confusion regarding which NRC office is responsible for ensuring adequate security measures are in place for contractor-operated systems, especially Web applications. As previously stated, the inventory of Web applications provided by NRC was incomplete. In addition, some Web applications did not have an apparent system owner and could not be identified as belonging to any of NRC's approved system authorization boundaries. The evaluation team had particular difficulty in identifying responsible offices/system owners for contractor-operated Web applications.

Why This Is Important

Security Measures May Not Be Adequate to Reduce Risk of Compromise

The configuration of an information system and its components has a direct impact on the security posture of the system. System changes can adversely affect the previously established security posture; therefore, effective configuration management and patch management are vital to the establishment and maintenance of security of information and the

information system. For example, three of the Web applications tested did not sufficiently sanitize input that can be edited by a user. Processing unsanitized input could result in data loss, data corruption, unauthorized access, or harm to the organization's reputation.

If configuration management and patch management procedures are not consistently implemented, information security protections may not be commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of NRC information and information systems.

Recommendation

OIG recommends that the Executive Director for Operations

5. Develop a plan and schedule for evaluating the vulnerabilities identified, determining the appropriate action to address the vulnerability (e.g., mitigation, deviation, risk acceptance), and implementing the remedial actions.

D. Authorization to Operate the NRC Webcast Portal Did Not Follow the NRC RMF Process

The Federal Information Security Modernization Act of 2014 (FISMA 2014)[4] requires agencies to ensure the adequate protection of agency information, including information collected or maintained by contractors, as well as information systems operated by contractors on the agencies' behalf. NRC has policies for performing oversight of contractor systems. However, the evaluation team found that authorization to operate the NRC Webcast Portal did not follow the NRC RMF process. As a result, NRC is unable to determine whether adequate security measures are in place to reduce the risk of compromise for the NRC Webcast Portal.

[4] FISMA 2014, signed December 18, 2014, reformed the Federal Information Security Management Act of 2002 (FISMA).

What Is Required

Federal Requirements for Oversight of Contractor Systems

FISMA 2014, Section 3554(a)(1)(A)(ii) describes Federal agency security responsibilities as including "information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." Section 3554(b) requires each agency to provide information security for the information and "information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source." This includes services that are provided (in full or in part) by another Federal agency, outsourced to a commercial vendor, and cloud solutions such as software-as-a-service.

Agencies are fully responsible and accountable for ensuring all FISMA and related policy requirements are implemented and reviewed for all contractor systems. Agencies must ensure identical, not "equivalent," security procedures. For example, annual testing and evaluation, risk assessments, security plans, security control assessments, contingency planning, and security authorization must also be performed for all contractor systems.

Internal Guidance Regarding Oversight of Contractor Systems

Management Directive and Handbook 12.5, *NRC Cyber Security Program*, require Federal agencies or third-party service providers hosting NRC capabilities to meet NRC cyber security requirements. CSO-PROS-2030 describes the process for applying the RMF described in NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, to secure NRC systems, including contractor systems. It specifies the steps required to obtain IT system authorization and authorization requirements for IT systems, applications, laptops, services, and facilities.

Per CSO-PROS-2030, the NRC Webcast Portal would be considered a "Service" that is not operated by another Federal agency. Therefore, it must be authorized to operate by NRC as an IT system.

NRC Webcast Portal Contract and Statement of Work

The following IT security requirements were specified in the contract[5] for the NRC Webcast Portal:

- Contractor shall complete a security survey of the proposed facility in accordance with Management Directive and Handbook 12.1, *NRC Facility Security Program.*
- Contractor shall perform a full certification and obtain accreditation of the facility and computing systems.
- Webcasting services provided by the contractor under this contract shall meet the cloud computing security requirements outlined by the Federal Risk and Authorization Management Program (FedRAMP).
- The NRC ISD will act as the third-party assessment organization and contractor solution must obtain an authorization to utilize from the NRC ISD.
- Within 90 calendar days of the date of the award, the contractor provides an updated IT Security Plan, based on the proposed draft IT Security Plan.

What We Found

NRC Webcast Portal Was Not Authorized to Operate

Despite NRC's requirements for authorizing the use of contractor systems, as well as the security requirements specified in the contract and statement of work for the NRC Webcast Portal, the evaluation team found that none of the required authorization activities was performed. NRC did provide an IT Security Plan for the NRC Webcast Portal (referred to in that document as the Online Video Service); however, the document is dated November 1, 2013, is marked as a draft, and is incomplete. Testing of the

[5] Contract NRC-HQ-13-C-10-0068, dated September 27, 2013. Period of performance: September 27, 2013 – February 28, 2014, plus 4 one-year option periods.

NRC Webcast Portal found vulnerabilities in four of the ten OWASP Top 10 categories.

Why This Occurred

An important cause for the lack of an authorization to operate is confusion regarding which NRC office is responsible for ensuring adequate security measures are in place for contractor-operated systems, especially Web applications. As previously stated, the inventory of Web applications provided by NRC was incomplete. In addition, some Web applications did not have an apparent system owner and could not be identified as belonging to any of NRC's approved system authorization boundaries. The evaluation team had particular difficulty in identifying responsible offices/system owners for contractor-operated Web applications.

Further, oversight of contractor systems was identified as a weakness in several past FISMA evaluations. For example, the fiscal year 2013 FISMA evaluation found that the inventory of contractor systems was incomplete, and the NRC RMF was not consistently followed for contractor systems. In September 2015, the agency reported that all RMF activities for contractor systems had been completed; however, the agency did not provide sufficient evidence that the recommendation was actually completed.

Why This Is Important

Adequacy of Security Controls for the NRC Webcast Portal Could Not Be Determined

Agencies are fully responsible and accountable for ensuring all FISMA and related policy requirements are implemented and reviewed for all contractor systems. Agencies must ensure identical, not "equivalent," security procedures. For example, annual testing and evaluation, risk assessments, security plans, security control assessments, contingency planning, and security authorization must also be performed for all contractor systems. However, as NRC did not perform these activities for the NRC Webcast Portal, the agency is unable to determine whether

adequate security measures are in place to reduce the risk of compromise.

Recommendation

OIG recommends that the Executive Director for Operations

6. Complete the appropriate NRC RMF authorization activities for the NRC Webcast Portal.

E. NRC'S IT System Decommissioning Process Needs Improvement

Federal guidance requires organizations to execute certain actions when a system is removed from service. A number of risk management-related actions are required, including updating organizational tracking and management systems (including inventory systems) to indicate the specific information system components that are being removed from service. NRC has developed a process for the orderly decommissioning and disposal of an unclassified IT system and any associated data that applies to any information system that stores, transmits, receives, or processes unclassified NRC data. However, the evaluation team found that retired IT systems are still allocated resources. For example, targets noted as retired were still included in the NRC's DNS and were provided as targets for DHS Cyber Hygiene scans. While exact reasons are difficult to determine accurately, possible causes include the fact that IP address space is readily available at NRC and decommissioning procedures may not have complete information on how IP address space should be decommissioned or which inventories need to be updated. Projects relying on outdated inventories and DNS entries mean that resources are repeatedly spent working on IP addresses that are not assigned to active hosts.

What Is Required

External Requirements for Decommissioning IT Systems

Step 6 of the NIST RMF, as described in NIST SP 800-37, requires organizations to implement an information system disposal strategy that

executes required actions when a system is removed from service. A number of risk management-related actions are required, including updating organizational tracking and management systems (including inventory systems) to indicate the specific information system components that are being removed from service.

Internal Requirements for Decommissioning IT Systems

CSO-PROS-2101, *NRC IT System Decommissioning and Disposal Process*, provides the process used for orderly decommissioning and disposal of an unclassified IT system and any associated data. The process applies to any information system that stores, transmits, receives, or processes unclassified NRC data.

System owners must formally notify the Director and Deputy Director, OCIO of the IT system's retirement within 5 days of Designated Approving Authority authorization. OCIO must be furnished with all necessary information and documentation to update the NRC system inventory. OCIO shall ensure the NRC system inventory is updated as appropriate.

System deactivation may not be performed prior to the communicated deactivation date. System owners shall ensure that proper resources are allocated to deactivate the system in a timely fashion. To deactivate the IT system, all components of the system shall be powered down and the system disconnected from all networks.

What We Found

Retired IT Systems Are Still Allocated Resources

The initial list of potential targets provided by NRC for this assessment included systems noted as retired. The DNS data later provided by NRC included entries for hosts that had been marked as retired in the initial list, indicating that retired hosts are not removed from DNS in a timely fashion. Other target data sources, including targets included in DHS Cyber Hygiene scans, and targets from a recent penetration testing engagement also included retired hosts and planned hosts that had never been placed in production, indicating that time and effort may have been spent testing allocated but unused IP addresses.

Why This Occurred

Exact reasons are difficult to determine accurately why retired IT systems are still allocated resources. Possible causes include the fact that IP address space is readily available at NRC and decommissioning procedures may not have complete information on how IP address space should be decommissioned or which inventories need to be updated.

Why This Is Important

Projects relying on outdated inventories and DNS entries mean that resources are repeatedly spent working on IP addresses that are not assigned to active hosts. Each project or project team would need to take time to confirm the IP addresses are not actually in use, causing an immeasurable amount of repeated work. It is highly likely that the level of effort required for NRC to maintain an accurate inventory is significantly less than the effort expended in repeatedly confirming which hosts are retired.

Recommendation

OIG recommends that the Executive Director for Operations

7. Update CSO-PROS-2101 to include procedures for updating DNS entries and other resources allocated to new systems in addition to the inventory.

IV. CONSOLIDATED LIST OF RECOMMENDATIONS

OIG recommends that the Executive Director for Operations

1. Develop and document procedures for ensuring publicly accessible Web applications are assigned a system owner with responsibility for ensuring adequate security measures are in place for those applications.

2. Develop and document procedures for ensuring publicly accessible Web applications are incorporated into an approved system authorization boundary and for clearly identifying those applications in system authorization documentation.

3. Develop and document procedures for ensuring DHS is notified of any changes to the population of publicly accessible Web applications to be included in the Cyber Hygiene scans.

4. Develop a plan and schedule to identify, review, and update all NRC cyber security standards that have not been updated in the past 12 months.

5. Develop a plan and schedule for evaluating the vulnerabilities identified, determining the appropriate action to address the vulnerability (e.g., mitigation, deviation, risk acceptance), and implementing the remedial actions.

6. Complete the appropriate NRC RMF authorization activities for the NRC Webcast Portal.

7. Update CSO-PROS-2101 to include procedures for updating DNS entries and other resources allocated to new systems in addition to the inventory.

V. AGENCY COMMENTS

An exit conference was held with the agency on May 18, 2016. Prior to this meeting, after reviewing a discussion draft, agency management provided comments that have been incorporated into this report, as appropriate. As a result, agency management stated their general agreement with the findings and recommendations in this report and opted not to provide formal comments for inclusion in this report.

Appendix

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The objective was to determine i) the effectiveness of NRC's efforts to secure its publicly accessible Web applications, and ii) whether NRC has implemented adequate security measures to reduce the risk of compromise for their publicly accessible Web applications.

Scope

The evaluation focused on identifying the target population of publicly accessible Web applications and performing a vulnerability assessment of those targets, with the option for attempting to exploit identified vulnerabilities, if requested. The testing was performed to identify potential vulnerabilities in NRC publicly accessible Web applications that may be vulnerable to exploitation by threats through the Internet.

The evaluation was performed with the full cooperation of NRC. NRC perimeter security services (e.g., firewalls, intrusion detection/prevention systems) were configured to whitelist (i.e., monitor only, not block) the scanning platforms/hosts identified in the agreed upon rules engagement. The evaluation team did not make any attempts to test the effectiveness of such perimeter security services.

The evaluation was conducted at NRC headquarters (Rockville, MD) from November 2015 through April 2016. Any information received from the agency subsequent to the completion of fieldwork was incorporated when possible. Internal controls related to the evaluation objective were reviewed and analyzed. Throughout the evaluation, the evaluation team was aware of the possibility of fraud, waste, and abuse in the program.

Methodology

To conduct the evaluation, the team conducted the following activities:

- Interviewed agency IT security personnel and contractors in charge of Web management and/or security.

- Tested systems and management consoles on NRC networks that are publicly accessible.

- Used a number of techniques to quantify the number of agency IP addresses associated with publicly accessible Web applications and link the IP addresses back to system security plans to determine system impact levels.

In addition, the team reviewed the following documentation:

- NRC policies, procedures, and guidance specific to NRC's IT security program.

- NRC policies, procedures, and guidelines specific to application development, Web application development, and external Web pages.

- Contract documents for contractor systems with publicly accessible Web applications identified during the evaluation.

- System security plans for NRC and contractor systems with publicly accessible Web applications identified during the evaluation.

All analyses were performed in accordance with guidance from the following:

- NRC OIG contract and guidance.

- NIST standards and guidelines.

- U.S. Computer Emergency Readiness Team guidance.

- Guidance published by the Open Web Application Security Project.

- Guidance published by the SANS Institute.

- Council of the Inspectors General on Integrity & Efficiency, *Quality Standards for Inspection and Evaluation*, January 2012.

- Management Directive and Handbook 12.5, *NRC Cyber Security Program*.

- NRC Information Security Directorate policies, processes, procedures, standards, and guidelines.

- Guidance issued by the CIGIE Web applications crosscutting project working group.

The evaluation was conducted by Jane Laroussi, CISSP, CAP; Matt Brincefield, CISSP, GWAPT, GPEN; Antoine White, CISA; and Diane Reilly, Senior Vice President/Project Manager, from Richard S. Carson & Associates, Inc. The evaluation was performed under contract #GS00F0001N NRC-HQ-30-15-T-0001, on behalf of NRC OIG Security and Information Management Audits team. Beth Serepca is Team Leader, and Amy Hardin was Contracting Officer's Representative.

TO REPORT FRAUD, WASTE, OR ABUSE

Please Contact:

Email:	Online Form
Telephone:	1-800-233-3497
TDD	1-800-270-2787
Address:	U.S. Nuclear Regulatory Commission Office of the Inspector General Hotline Program Mail Stop O5-E13 11555 Rockville Pike Rockville, MD 20852

COMMENTS AND SUGGESTIONS

If you wish to provide comments on this report, please email OIG using this link.

In addition, if you have suggestions for future OIG audits, please provide them using this link.