UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

Washington, DC 20415

Chief Information Officer

MEMORANDUM FOR ASSOCIATE DIRECTORS AND OFFICE HEADS

THROUGH: GUY CAVALLO
Acting Chief Information Officer
Office of the Chief Information Officer

Guy Cavallo Digitally signed by Guy Cavallo Date: 2021.06.10 17:10:12 -04'00'

FROM: CORD E. CHASE
Chief Information Security Officer
Office of the Chief Information Officer

DARRIN MCCONNELL Digitally signed by DARRIN MCCONNELL Date: 2021.06.10 17:03:19 -04'00'
On behalf of Cord E. Chase

Subject: Vulnerability Disclosure Policy #CIO-CSP-FY21-01

1. Purpose/Objective

This policy provides requirements for Vulnerability Disclosure for Office of Personnel Management (OPM) managed external-facing Dot-Gov (.gov) websites.

2. Authorities

The authorities for this policy include:

A. Federal Information Security Modernization Act of 2014 (P.L. 113-283), December 2014[1]

B. Federal Information Processing Standards Publication 200, March 2006[2]

C. Office of Management and Budget Circular A-130, July 2016[3]

D. Office of Management and Budget Circular M-20-32, September 2020[4]

E. Department of Homeland Security (DHS) Binding Operational Directive (BOD) 20-01, September 2020[5]

---

[1] https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf

[2] http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

[3] https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf

[4] https://www.whitehouse.gov/wp-content/uploads/2020/09/M-20-32.pdf.

[5] https://cyber.dhs.gov/bod/20-01/

3. Scope

This policy applies to all Office of Personnel Management (OPM) information systems and services with an external facing dot-gov (.gov) domain name.

4. Definitions

A. Chief Information Security Officer (CISO): The CISO carries out the responsibilities of the Chief Information Officer (CIO) under the Federal Information Security Modernization Act of 2014 (FISMA).

B. Infrastructure/Cloud Manager (ICM): Manages the environment, data center, and/or cloud services that handles OPM applications or data, at all locations where it is maintained, and is responsible for providing in-depth information security support for OPM's IT environments.

C. System Owner (SO): The program manager responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of information system. The SO is responsible for supporting the OPM mission and compliance with information security requirements of an information system.

D. Security Operations Center (SOC): The SOC is responsible for the development, primary component of OPM's Incident Response Plan. The SOC is the primary component of OPM's incident response capabilities, including monitoring, handling, and response, and supports the SO with technical security support.

5. Roles and Responsibilities

A. The CISO must:

1. Develop, publish, and maintain a Vulnerability Disclosure Policy.

B. Infrastructure/Cloud Managers must:

1. Identify and report to the CISO and SOC information systems and/or services that meet the criteria established under this policy (external facing OPM registered and managed .gov domains).
2. Manage the OPM Internet Domain Information and Root as identified in this policy.

C. System Owners must:

1. Identify to the Infrastructure/Cloud Manager any information system and/or services that are resources that meet the criteria established under this policy (external facing OPM registered and managed .gov domains).
2. Remediate vulnerabilities as identified by the SOC.

D. Security Operations Center must:

1. Monitor the Vulnerability Disclosure email for VDP Reports.
2. Perform review of VDP Reports and pass on acceptable reports for analysis.
3. Perform initial analysis of vulnerabilities reported and make recommendations for remediation.
4. Report to VDP initiators, as necessary, the acceptance and remediation of identified vulnerabilities.

6. Policy

In addition to the roles and responsibilities described within this policy, the following security requirements must be met to secure OPM information systems. The security requirements below are described within the DHS BOD.

A. CISO Requirements:

BOD-ACTION	REQUIREMENT
3.a	Develop and Publish a Vulnerability Disclosure Policy.
3.c	Every three years review and, if necessary, update the Vulnerability Disclosure Policy. Changes should appropriately be published to each external facing OPM registered and managed .gov domains.
8.a	Immediately report to CISA any valid/credible Vulnerability Reports for newly discovered or not publicly known vulnerabilities (including misconfigurations) on agency systems that use commercial software or services that affect or are likely to affect other parties in government or industry.
9.a	On a quarterly basis, in the agency's CyberScope Report include the captured Vulnerability Disclosure metrics.

B. Infrastructure/Cloud Managers Requirements:

BOD-ACTION	REQUIREMENT
1.a	For each external facing OPM registered and managed .gov domain, assure that the "Security Contact" field is set to the Security Contact email address (vulnerabilitydisclosure@opm.gov).
1.c	Review and update the external facing OPM registered and managed .gov domains information on an annual basis or when changes occur.
2.a	For each external facing OPM registered and managed .gov domain, assure that the "Organization" field is set to the agency component responsible for the internet-accessible services offered at the domain. If the domain is for a general or agency-wide purpose, use the most appropriate descriptor. This value should usually be different from the value in the “Agency” field.
3.b	For each external facing OPM registered and managed .gov domain publish the vulnerability disclosure policy as a public web page in plain text or HTML at the “/vulnerability-disclosure-policy” path.
4.c	All newly launched internet-accessible systems or services must be included in the scope of the policy. If the policy’s scope does not implicitly include the new system or service, the policy must be updated to include the new system or service explicitly.

C. Security Operations Center Requirements:

BOD-ACTION	REQUIREMENT
7.a	Develop or update vulnerability disclosure handling procedures to support the implementation of the VDP.
7.b	On an annual basis review and, if necessary, update the Vulnerability Disclosure Handling Procedures.

D. System Owner Requirements:

BOD-ACTION	REQUIREMENT
1.b	Identify all current internet-based web systems and services to the Infrastructure/Cloud Manager.
4.a	Identify, prior to implementation, any new internet-based web systems and services to the Infrastructure/Cloud Manager.
4.b	Identify any changes to currently identified internet-based web systems and services to the Infrastructure/Cloud Manager, including revocation and disposal.

7. Compliance, Enforcement, and Exceptions

The OPM sanctions process is applicable to all OPM employees, contractors, fiscal agents, financial agents, and subcontractor personnel who handle or access OPM information systems and equipment where OPM information is processed, transmitted, and stored.

A. Compliance: This OPM security policy is mandatory for all employees and contractors. This policy uses the plain language guidelines for conveying requirements. The following convention is used:

- “must” for an obligation;
- “must not” for a prohibition;
- “may” for a discretionary action; and
- “should” for a recommendation.

B. Enforcement: A policy violation is an infringement or nonobservance of OPM policy. If a policy violation is suspected, OPM employees must report it to their OPM supervisor, manager, associate director, or office director, as appropriate. The Chief Information Security Officer (CISO) may take technical, preemptive actions to isolate the suspected violators and systems to prevent additional risk to OPM. Violations of this policy may result in one or more of the following:

- Counseling;
- Suspension of access privileges;
- Termination of employment;
- Financial liability; and / or

- Criminal charges.

C. Exceptions: Policy waivers are approved deviations from a policy requirement that are only allowed when adherence to the policy is not feasible. The CISO maintains the formal request form, which must be submitted by Office Heads and / or Leadership to the CISO for review and approval. Each waiver must be submitted with a compelling business case justification and risk assessment. Waivers will be reviewed on a case-by-case basis. Waivers granted for an information system will remain valid until the Authorization to Operate for the system expires. Waivers granted for an office will remain valid until the next review and update of the policy occurs.

8. Contact Information

Any questions or concerns regarding this policy should be directed to:

- Policy Owner: OPM Chief Information Security Officer
- IT Security (Policy): CyberSolutions@opm.gov

9. Expiration and Renewal

This policy is in effect as of 03/01/2021. This policy must be reviewed and renewed every three years.

Appendix A Website Root Page Content

The following content will be published to each OPM .gov website on the root "/vulnerability-disclosure-policy/" location:

OPM Vulnerability Disclosure Process

1. Introduction

As part of a U.S. government agency, the Office of Personnel Management (OPM) takes seriously our responsibility to protect the public's information, including financial and personal information, from unwarranted disclosure.

We want security researchers to feel comfortable reporting any vulnerabilities they discover, as set out in this policy, so that we can fix them and keep our information safe.

This policy describes what systems and types of research are covered under this policy, how to send us vulnerability reports, and how long we ask security researchers to wait before publicly disclosing any vulnerabilities.

OPM encourages you to contact us to report potential vulnerabilities in our systems.

2. Authorization

If you make a good faith effort to comply with this policy during your security research, OPM will consider your research to be authorized. OPM will not pursue legal action against authorized research.

3. Guidelines

We require that you:

- Notify us as soon as possible after you discover a real or potential security issue.
- Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data.
- Only use exploits to the extent necessary to confirm a vulnerability. Do not use an exploit to compromise or exfiltrate data, establish command line access and/or persistence, or use the exploit to "pivot" to other systems.
- Once you have established that a vulnerability exists, or encountered any of the sensitive data (including personally identifiable information, financial information, or proprietary information or trade secrets of any party), you must stop your test and notify us immediately, and not disclose this information to anyone else.
- Provide us a reasonable amount of time to resolve the issue before you disclose it publicly.
- Keep confidential any information about discovered vulnerabilities for up to 90 calendar days after you have notified OPM.

4. Scope

This policy applies to the following domains:

- External facing OPM registered and managed .gov domains and all sub-domains (e.g. telework.opm.gov),

- applicationmanager.gov,
- chcoc.gov,
- cybercareers.gov,
- employeeexpress.gov,
- feb.gov,
- federaljobs.gov,
- fedjobs.gov,
- fedshirevets.gov,
- fsafeds.gov,
- golearn.gov,
- governmentjobs.gov
- opm.gov,
- pac.gov
- pmf.gov
- telework.gov,
- unlocktalent.gov
- usajobs.gov,
- usalearning.gov
- usastaffing.gov
- Non-public data on public third-party services - OPM utilizes third-party services to support its public work model. While non-public data published publicly on those services is in scope, testing those services is **not** in scope.

Any services not expressly listed above, such as any connected services, are excluded from scope and are not authorized for testing. Additionally, vulnerabilities found in non-federal systems from our vendors fall outside of this policy's scope and should be reported directly to the vendor according to their disclosure policy (if any). If you are not sure whether a system or endpoint is in scope or not, contact us at vulnerabilitydisclosure@opm.gov before starting your research.

OPM does not offer any compensation for the identification or reporting of vulnerabilities.

5. Test methods

Security Researchers/Testers must not:

- Perform testing of any information system or service unless it is in the Scope of this policy;
- Perform any Denial of Service (DoS or DDoS), Resource Exhaustion, or other tests that impair access to an information system or data (information);
- Preform physical testing (e.g. office access, open doors, tailgating) of federal/contractor facilities or resources;

- Perform social engineering (e.g. phishing, vishing), or any other non-technical vulnerability testing to include the sending of unsolicited emails;
- Introduce any malicious software/code;
- Perform testing in a manner which could degrade the operations of systems, or intentionally impair, disrupt, or disable information systems or services;
- Preform testing on third-party applications, websites, or services that integrate with or link to or from agency information systems or services;
- Perform testing that intentionally or unintentionally deletes, alters, shares, retains, or destroys information (data);
- Perform testing of an exploit to exfiltrate data, establish command line access, elevate privileges, establish a persistent presence on systems, or "pivot" to other systems;
- Perform testing that maintains a persistence presence on information systems or services.

Security Researchers/Testers must:

- Cease testing and notify us immediately upon discovery of a vulnerability;
- Cease testing and notify us immediately upon discovery of an exposure of nonpublic data to include Personally Identifiable Information (PII), Financial information (e.g. credit card or bank account numbers), and Proprietary information or trade secrets of companies of any party;
- Purge any stored agency nonpublic data upon reporting a vulnerability.

6. Reporting a Vulnerability

- We accept vulnerability reports using the provided reporting format via the following methods:
- Email: All submission via email will be sent to vulnerabilitydisclosure@opm.gov.

The Vulnerability Report should be in the template provided. Vulnerability Reports that are not in the correct template or that do not provide sufficient information will be rejected for processing by the analysis team.

Please note that Vulnerability Reports may be submitted anonymously. If you share contact information (Reporter Contact), we will acknowledge receipt of your report within five (5) business days of the reports receipt.

We do not support PGP-encrypted emails. For particularly sensitive information, submit through the mail process or provide a note that some information is sensitive, and you will be contacted with details on sending the sensitive information.

A. What we would like to see from you:

In order to help us triage and prioritize submissions, we recommend that your reports:

- Describe the location the vulnerability was discovered and the potential impact of exploitation.
- Offer a detailed description of the steps needed to reproduce the vulnerability (proof of concept scripts or screenshots are helpful).

- Be in English, if possible.

B. What you can expect from us:

- When you choose to share your contact information with us, we commit to coordinating with you as openly and as quickly as possible.
- Within three (3) business days, we will acknowledge that your report has been received.
- To the best of our ability, we will confirm the existence of the vulnerability to you and be as transparent as possible about what steps we are taking during the remediation process, including on issues or challenges that may delay resolution.
- We will maintain an open dialogue to discuss issues.

Appendix B Reporting Format

The following format should be utilized for reporting vulnerabilities to OPM:

Office of Personnel Management Vulnerability Disclosure Form

1. **Using This Form**

   All information fields with an asterisk (*) are required for the processing of this Vulnerability Disclosure Form, all other fields are optional. If the required fields are not complete, the Vulnerability Disclosure Form may not be processed. When complete submit the completed Vulnerability Disclosure Form to:

   EMAIL: vulnerabilitydisclosure@opm.gov

   SUBJECT: Vulnerability Disclosure Report

2. **Vulnerability Information**

   - Website Uniform Resource Locator (URL) (e.g. www.opm.gov)?*
   - Website/Application Internet Protocol (IP) Address (IP4/IP6)?
   - Website/Application/Software Name?
   - Website/Application/Software Version?
   - Access Method (e.g. Firefox, IE, Chrome)?
   - Describe the vulnerability discovered?*
   - What date was the vulnerability discovered?*
   - How was the vulnerability discovered?*
   - Detail the steps taken to discover the vulnerability?*
   - What testing method(s) were used to discover the vulnerability?
   - What testing tools were used to discover the vulnerability?
   - Is the vulnerability discovered publicly known (Yes/No)?
   - Common Vulnerabilities and Exposures (CVE) Number?
   - Was there any exposure of Personally Identifiable Information (PII) (Yes/No)?

- Was there any exposure of Financial Information (Yes/No)?
- Was there any exposure of Proprietary or Sensitive Information (Yes/No)?

3. Contact Information

- Contact Name?
- Contact Email?
- Contact Phone Number?
- Do You Wish To Remain Anonymous (Yes/No)?*

4. Questions

Questions regarding this policy may be sent to vulnerabilitydisclosure@opm.gov.