GUIDE TO VULNERABILITY REPORTING FOR AMERICA'S ELECTION ADMINISTRATORS

INTRODUCTION Meet Security Researchers

America expresses itself through its elections. Citizens expect the same speed, security, and accuracy in voting as they expect in their communications. Even when we cast a paper ballot at a polling place, election officials rely on dozens of electronic data systems to bring the right ballots to each registered voter and to ensure they are accurately counted.

Like other electronic systems, risk to election systems can be effectively managed, but vulnerabilities do exist. Election administrators should know that the cybersecurity research community can help ensure these systems are safe so that the choices of the voting public can be clearly heard. This Guide offers a step by step guide for election administrators who seek to establish a successful vulnerability disclosure program.

- As election administrators, you already trust members of the public with extremely sensitive election tasks from voter registration to poll book/ID checks to vote counting.
- Free and fair elections are a key component of our democracy, and we all have a role to play in keeping them safe from interference.
- Cybersecurity Researchers who follow vulnerability disclosure policies can help you keep elections safe.

To take advantage of input from Cybersecurity Researchers, you will need to:

1. Clearly identify the systems on which you would permit them to conduct testing.
2. Detail the nature of permissible testing in writing.
3. Define a point of contact.
4. Have resources (including personnel) to vet and fix the issues they report while keeping them informed.

Who are Cybersecurity Researchers?

- While they are diverse in motivations and capabilities, legitimate security researchers are people who test websites, systems, software, and hardware for vulnerabilities that:
  - Could be exploited to make them operate in a manner its operator did not intend.
  - Could compromise the confidentiality, integrity, or availability of information.
  - Could help the researcher understand how websites, systems, software, or hardware products function or are designed.
- Cybersecurity Researchers have various goals: “presume benevolence” (see CERT-CC guide) when researchers comply with authorized testing policies.
  - Many researchers are professionals who seek to advance computer science as an academic discipline, create business for a cybersecurity company, or earn bug bounties.
  - Others are hobbyists who volunteer to help organizations avoid exploitation.
  - Some are people who simply see a website or product act in a concerning way.

- **Cybersecurity Researchers often use the same tactics as a malicious attacker with the goal of identifying vulnerabilities that malicious attackers could exploit.**
- **Legitimate security researchers differ from malicious attackers in that ethical researchers report their findings to help fix them and have no intent to use the information for illicit purposes.**
    - Proponents of Coordinated Vulnerability Disclosure often cite these ethical norms:
        - Attempt to help the affected entity fix vulnerabilities before public disclosure.
        - Do not disclose data accessed in the course of testing to third parties.
        - Publish findings to help others fix the same issue.

What Can Cybersecurity Researchers Do To Help Me?

- **Find and report security issues to you before tampering can occur.**
- **Connect you with others in the research community who might be able to offer assistance.**
- **Types of Issues:**
    - Network and device misconfigurations (which often make data accessible remotely). This includes sensitive data accessible outside a firewall and network adapters enabled on isolated devices.
    - Application-layer vulnerabilities or poor security controls including default/no password set for access to databases, or poor data sanitization on webforms.
    - Devices that contain known security vulnerabilities.
- **Remember, if someone reports a security issue in your network, a malicious actor can find it too.**

TABLE OF CONTENTS

STEP 1 Identify Systems Where You Would Accept Security Testing, And Those Off-Limits

- **Each of America's thousands of states and local election jurisdictions is a little different, but each conduct similar core functions which often have some electronic support:**

- Voter registration and voter registration verification
- Keeping voters informed about where, when, and how to vote
- Distribution of the correct ballots to the correct people/places
- Voter check-in and (sometimes) ID validation
- Vote tabulation and reporting
- Post-election audits
- Allocation of registered voters to districts and polling places, building poll books
- Managing poll workers
- Configuring voting machines and tabulation/ballot storage devices
- Voting!
- Election night reporting

CONSIDER THE ELECTRONIC SYSTEM USED AT EACH STAGE AND HOW THEY WORK TOGETHER

Identify (privately) the systems which should be connected to the **public internet**

Identify (privately) the systems which should only connect to **each other**

Identify (privately) the systems which should be **isolated from a network**

- **Security researchers often find these things are connected in unexpected ways, or that organizations' asset inventories are incomplete (with uneven protections for systems).**

- **Consider whether your election organization uses managed service providers, Software-as-a-Service contractors, or other electronic infrastructure platforms to fulfill core functions:**

    - Third party systems and their interconnections with your organization's own systems are a critically important part of the risk to your operations.
        - Election technology vendors on contract to state and local governments are responsible for many critical parts of election systems whose design and code require advance certification by the U.S. Election Assistance Commission before use in federal elections.
        - While state and local governments have legal authority to designate the systems and networks they own for vulnerability testing in order to reduce risk to their missions, the certification requirement for election systems may mean that expansion of public vulnerability disclosure and testing policies to systems operated under contract may take significant advance planning.

    - Ensure that you have the legal authority to authorize security testing on the networks or devices owned by third-party entities before including them in your policy.
        - Election organizations may be able to negotiate this into contracts with vendors.
        - Your organization can approach your vendors regarding their willingness to authorize testing if the existing contract is unclear on this point.
        - Some commonly used providers have posted a publicly posted policy on security testing of their services.
        - If the vendor is unwilling to authorize public security testing, ensure that relevant IP ranges, subdomains, and other systems are clearly out of scope in your policy.

- **Identify which systems, domains, and IP ranges you would accept testing for security vulnerabilities.**

    - If a resource is designed for public access (e.g. your website), testing is simple.
        - Many vulnerability disclosure policies simply list domains and subdomains, sometimes with a wildcard operator (i.e. * .elections.state.gov).
        - Specific systems on these domains can still be identified as out of scope in your policy.
    - Researchers can also let you know when things that should **never be accessible** are accessible!
    - More complex are attempts to map your network, or find voter data on cloud services.

STEP 2 Draft An Easy-to-Read Vulnerability Disclosure Policy (See Appendix III)

- **A public Vulnerability Disclosure Policy allows each election administrator to set rules for authorized testing, creating a guide to their relationship with security researchers.**
- **Organizations that seek to authorize testing of their internet connected systems usually publish a Vulnerability Disclosure Policy on a public website that can easily be located from the organization's homepage or by a web search.**
- **Consider that security researchers have different motivations underlying their work, which will lead them to expect different things from you.**

- **Vulnerability Disclosure Policies include, at a minimum, these core items:**

1. Which systems, IP ranges, sites, and/or data storage elements are authorized for testing.
2. Which types of testing are allowed or prohibited.
3. An explicit statement prohibiting disclosure of any personally identifiable information or non-public data to any third party.
4. A description of how to submit vulnerability reports, which should include:
    a. How/where to submit a report (i.e. an email address or secure web service) and an encryption key for email.
    b. A request for information (known as "proof of concept") needed to find and analyze the vulnerability.
        i. A description of the vulnerability and its technical impact.
        ii. The physical device or internet location where it exists.
        iii. Technical information needed to reproduce, including screenshots or text of any proof of concept code.
    c. A statement permitting researchers to submit anonymous reports.
    d. A request for the submitter's contact information and permission to follow up with technical questions (but consider if your state and local privacy laws permit exemptions of personal contact information from freedom of information act requests).
5. A public statement that your organization:
    a. "Will not recommend or pursue legal action" against anyone for security research activities that represent, in your organization's view, a good faith effort to follow this policy.
    b. That such activities are "deemed to be authorized."
6. A date of issuance.

- **Vulnerability Disclosure Policies may include these items at your discretion:**

1. A statement that your organization will acknowledge all submissions by return email (where provided) within a certain number of days.
    - Seven days is standard for a personal response, 24 hours for an automated response.
    - Most vulnerability disclosure programs assign a ticket number for tracking purposes.
2. If applicable, a statement that your organization will communicate with the submitter if their assistance is needed to reproduce or fix the issues, and they have provided a method of return communication.
3. A statement that your organization will thank the submitter when the issue is believed to have been resolved.
4. A request that submitters do not provide a specified high volume of reports per day/week (i.e. more than 25), or automated reports such as the output of scans.
5. A statement that submissions may be shared with other government election or cybersecurity agencies, or with product vendors, for the sole purpose of mitigating the identified risk in electronic systems.
6. A request that any previously undiscovered product security vulnerabilities ("zero-days") be disclosed to the product vendor or an established third-party coordinator.

- **Other Things to Consider When Structuring Your Vulnerability Disclosure Policy:**
    - Many organizations explicitly prohibit social engineering (such as phishing), which is often employed in legitimate commercial penetration testing.
    - Organizations may choose to place certain sensitive systems out of scope.
    - Researchers may be able to view sensitive information in the course of identifying security vulnerabilities:
        - Many policies state that researchers should not modify or access data beyond that necessary to demonstrate proof of concept.
        - Most policies explicitly prohibit sharing of such data with any third party.

- **Because many security researchers are professionals seeking name recognition, non-disclosure agreements that prevent them from discussing their work after the issue is fixed may deter them from assisting your organization.**

- **Organizations may consider paying a "bug bounty," (i.e. a reward for reported, validated vulnerabilities).**

    a. These programs encourage a higher number of researchers to initiate testing.

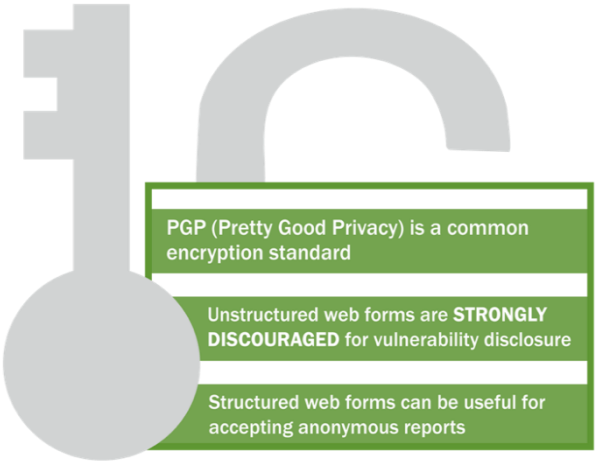
    b. Bug bounty programs can also increase the resources (in terms of staff time and program dollars) necessary to maintain a program.

    c. Many organizations initially operate their vulnerability disclosure program without offering financial compensation to researchers while they build their own capacity to patch identified issues and communicate with researchers.

STEP 3 Establish a Way to Receive Reports/Conduct Follow On Communication

- Before publishing a Vulnerability Disclosure Policy, your entity should establish a method of receiving unsolicited reports about potential cybersecurity vulnerabilities.
- This is typically, but not always, a generic email address on your organization's domain which can be accessed by multiple officials (some organizations use an intake webpage).

The intake email address or page should offer a public encryption key to secure data submissions, and the officials who access these messages should hold a private key



- You may consider having separate "Security@" and "Vulnerabilities@" addresses to ensure information about live security incidents is read immediately.
- If your organization has a .gov domain, consider updating your security contact information on the .gov registrar, ensuring that it is a regularly monitored generic email address.
    - If your organization has a .gov domain, you should register your security contact email address on dotgov.gov; this allows security researchers who identify issues connected to your domain to contact you.
- Your entity should also establish group email addresses for follow-on communication with researchers that are separate from individual officials' email addresses.
    - Security researchers will expect recipients of vulnerability reports to remain in contact, and a shared account permits tracking and status update responsibilities to be distributed among multiple officials.
    - A shared account also ensures officials' individual work email accounts are available for other routine business (requests for updates can be frequent).

STEP 4 Assign Someone to Thank and Communicate with Researchers

- Vulnerability coordination is as much about communication as technical fixes.
- Security researchers can help you discover weak points in your electronic systems and reduce the risk to your election operations.
- Security researchers are most likely to spot vulnerabilities in the systems of organizations that acknowledge their reports and set a reasonable expectation about two-way communication.

WHAT RESEARCHERS EXPECT OF YOU

SOME FORM OF RECOGNITION (OFTEN AS SIMPLE AS A THANK YOU EMAIL)

IN MOST CASES, THEY WANT TO KNOW THAT YOU RECEIVED THEIR MESSAGE AND WHETHER TO EXPECT FURTHER COMMUNICATION

THEY OFTEN WANT TO MAKE SUGGESTIONS TO HELP YOU FIX THE ISSUE (A GOOD TRAINING EXPERIENCE FOR YOUR IT STAFF)

IF POSSIBLE, CREDIT BY NAME OR PSEUDONYM IN A PUBLIC ANNOUNCEMENT FOR PROFESSIONAL DEVELOPMENT (SOME WILL WISH TO REMAIN ANONYMOUS)

SOME VULNERABILITY RESEARCHERS WILL WANT YOUR APPROVAL TO PUBLISH THEIR FINDINGS (HOW THE ISSUE WAS DISCOVERED AND FIXED) AFTER YOU FIX IT-AGAIN, TO BOLSTER THEIR ACADEMIC OR PROFESSIONAL CREDENTIALS

THIS IS WHY IT IS IMPORTANT TO OFFICIALLY DECLARE THE ISSUE "CLOSED" IN AN EMAIL

MOST RESEARCHERS TESTING ELECTION SYSTEMS ARE NOT LOOKING FOR MONEY (UNLESS A BUG BOUNTY PROGRAM EXISTS)

ACADEMIC RESEARCHERS ARE OFTEN BARRED FROM ACCEPTING OUTSIDE COMPENSATION

- According to a 2016 survey, 57% of researchers expected to be involved in testing mitigation of identified vulnerabilities and 53% expected acknowledgement[1].
- As many as 50% of researchers also considered public disclosure before the issue was fixed due to frustration working with a system owner, according to the same survey.

[1] U.S. Department of Commerce, National Telecommunications and Information Administration (NTIA), Multi-Stakeholder Awareness and Adoption Group Report: Vulnerability Disclosure Attitudes & Actions, 2016

STEP 5 Assign Someone to Vet and Fix the Vulnerabilities

A vulnerability mitigation program requires more than a disclosure policy; it requires staff time to vet and fix the issues and to keep the researchers informed (if not involved).

STEPS

1 Intake & Triage

- Your organization's staff or a third-party contractor review new vulnerability reports and conduct initial screening of plausibility.
- If a report appears to plausibly represent a security concern, triage staff assign a "ticket" to someone responsible for managing the affected item or system.
- Your staff sends an acknowledgement message to researchers who provide contact information usually using stock language.
    - If a report does not appear useful, the initial response thanks the researcher for their help and "closes the case," with a "no further action will be taken" statement.
    - If a report merits further action, the initial response should indicate that you may follow up with further questions and will notify them when fixed.

2 Discuss & Fix

- Your organization's IT staff prioritize vulnerabilities in need of patching, re-configuration, or other action in order of risk to your mission.
- As your IT staff attempt to fix the reported issue, they may need to ask the researcher for help reproducing the problem or testing whether it is fixed.

3 Closing A Case

- When your organization is done working on an issue, close the "ticket" and send your thanks in a message to the researcher (if possible).
- Some organizations send a bumper sticker, key chain, or other token gift to researchers who are especially helpful in reporting or fixing issues.
- Vendor organizations often publish a public security bulletin crediting researchers who seek acknowledgement.
- **IMPORTANT:** Researchers will take this final message as approval to publish a description of their findings, their methods of testing, and, sometimes, your emails to them to a public audience unless you have agreed otherwise.

STEP 6 Consider Sharing Information With Other Affected Parties

- **Many election administrators use similar combinations of hardware and software, and all are threatened by the same malign actors who seek to harm public trust in the voting process.**
    - If you believe that an issue reported with your systems could affect other election administrators, and your legal obligations permit, you should consider sharing a summary of the vulnerability and mitigation with other entities.
    - If a researcher reports a vulnerability to you which relates to a design defect in the software or hardware of a product and you believe it is "novel" (i.e. not known to the manufacturer), you should consider sharing the information with the manufacturer or a third party coordinator such as the Cybersecurity and Infrastructure Security Agency (CISA).
    - Your state board of elections, the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC), CISA, and the Election Assistance Commission (EAC), can help.
- **Public disclosure of things you have fixed contributes to a sense among citizens that you are in control of your cybersecurity risk, and helps manage the message.**

APPENDIX I. Difference Between "Zero-Day Vulnerabilities," Standard Security Vulnerabilities, and Bugs

- **Virtually all vulnerabilities disclosed to election administrators will be standard security vulnerabilities which can be fixed without a complex coordination process.**

- **Fixing security vulnerabilities = FIRST AID.**
- **Fixing zero-day vulnerabilities = DEVELOPING A CURE FOR A NEWLY DISCOVERED DISEASE (call a specialist).**

- **This analogy breaks down when election administrators have proprietary or custom systems built by vendors who have gone out of business, or when cloud computing and SaaS providers are involved.**
  - These issues are beyond the scope of this document, but require further discussion.

- **In increasing order of severity:**
  - **Bugs** are errors in the design or functioning of a software or hardware problem that cause it to behave in an unintended manner, but do not necessarily affect security.
  - **Security vulnerabilities** are common attributes of a hardware, software, process, or procedure that could enable or facilitate the defeat of a security control[2].
    - Security vulnerabilities permit negative effects to confidentiality, integrity, or availability of systems or data on those systems.
    - Security vulnerabilities can result from user misconfiguration, manufacturer error, or unanticipated problems in the interaction of items with each other.
      - Security vulnerabilities are common, widely known issues which can exist on a network.
      - When identified, security vulnerabilities can be fixed without a publication delay.
  - **Zero-day vulnerabilities** are weaknesses in the code of software and hardware components that are common to all copies of a particular version and are unknown to the vendor of the component.
    - Because these are latent/hidden vulnerabilities that can be exploited to harm virtually every user of a vulnerable item, it is critical that the manufacturer of the item has an opportunity to identify mitigation measures before public disclosure of the issue.
    - Zero-day vulnerabilities may affect a system component built into hundreds or thousands of different products, and delayed publication permits advance coordination.
    - Once mitigation/patch is available for a zero-day vulnerability, the public disclosure must be broadcast far and wide to prevent exploitation of users that have yet to fix it.

[2] See 6 U.S.C. 1501(17)

APPENDIX II. Background Resources To Consult (Additional Resources)

1. **For An Open-Source Perspective: [Disclose.io]'s USA Elections Core Terms**

2. **U.S. Department of Justice: Framework for a Vulnerability Disclosure Program for Online Systems (July 2017)**
   - A how-to guide to creating a vulnerability disclosure program which will encourage helpful conduct by security researchers and address issues under the Computer Fraud and Abuse Act.

3. **Carnegie Mellon University: Software Engineering Institute: CERT Guide to Coordinated Vulnerability Disclosure (September 2019)**
   - A troubleshooting and advice guide to communication with security researchers and coordinating vulnerability reports.

4. **Election Infrastructure Information Sharing and Analysis Center (EI-ISAC)**
   - A membership organization of election administrators which shares cyber risk management and threat information.

5. **CISA/Office of Management & Budget: Draft Binding Operational Directive 20-01, "Develop and Publish A Vulnerability Disclosure Policy" (November 2019 DRAFT)**
   - A draft Binding Operational Directive for U.S. Government Executive Branch Agencies requiring each to develop a program to receive and fix vulnerability issues identified by members of the public.

6. **Government of The Netherlands- Ministry of National Security: Responsible Disclosure Policy For Central Government Agencies**
   - An example of a long-standing and successful centralized vulnerability disclosure program for multiple entities within a government.

APPENDIX III. MODEL Vulnerability Disclosure Policy

- **The model vulnerability disclosure policy below was envisioned for a large federal agency with many web domains, IP ranges, and several layers of network operators.**

- **While it represents a best practice approach, a successful first attempt for a smaller entity with a less complex cyber architecture can be much less detailed.**

Vulnerability Disclosure Policy Template

This template is intended to assist your entity in the creation of a vulnerability disclosure policy (VDP) based on the federal agency standard in Draft Binding Operational Directive (BOD) 20-01

- *Instructions for how to use the template are provided throughout the document in **blue** and italic text and should be removed from your published policy.*
- *You are encouraged to modify the template to suit your needs. We **strongly recommend** that you use the template's language for the Authorization section.*
- *CISA recommends that you review the implementation guidance maintained in support of the directive concerning federal agency policies, particularly "Consider prior art."*
- *Your policy should be published as a web page and you should specify its location in your agency's security.txt.*

The primary sources for this template were the General Services Administration's Technology Transformation Services' VDP, the Department of Defense's VDP, and a VDP template from a 2016 working group of the National Telecommunications and Information Administration. It has been written to align with the Department of Justice's Framework for a Vulnerability Disclosure Program for Online Systems.

SAMPLE

Vulnerability Disclosure Policy

Entity Name

Month Day, Year

Introduction

An introductory section that provides background information about your organization and your VDP. It should take a committed, concerned, and receptive tone.

Entity Name is committed to ensuring the integrity of our elections by ensuring they are conducted without malicious interference or unwarranted disclosure of protected information. This policy is intended to give security researchers clear guidelines for conducting vulnerability discovery activities and to convey our preferences in how to submit discovered vulnerabilities to us.

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 vulnerabilities.

We want security researchers to feel comfortable reporting vulnerabilities they've discovered – as set out in this policy – so we can fix them and keep our users safe. We have developed this policy to reflect our values and uphold our sense of responsibility to security researchers who share their expertise with us in good faith.

Guidelines

Under this policy, research means activities in which 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's presence. 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.
- Provide us a reasonable amount of time to resolve the issue before you disclose it publicly.
- Do not submit a high volume of low-quality reports.

Once you've established that a vulnerability exists or encounter any sensitive data (including personally identifiable information, financial information, or proprietary information or trade secrets of any party), **you must stop your test, notify us immediately, and not disclose this data to anyone else.**

Authorization

This section reflects your commitment to not take legal action against anyone in the general public for security research activities that represent a good faith effort to follow the policy.

*CISA **strongly encourages** keeping this language as-is. The language is designed to be as welcoming to researchers as possible, and to avoid "legalese" or other unnecessarily intimidating language.*

If you make a good faith effort to comply with this policy during your security research, we will consider your research to be authorized and *Agency Name* will not recommend or pursue legal action related to your research. Should legal action be initiated by a third party against you for activities that were conducted in accordance with this policy, we will make this authorization known.

Scope

This section defines which internet-accessible systems or services are in scope of your policy. Your published VDP should offer researchers a system or service to test, and it should also describe the types of tests that are allowed (or specifically not authorized).

Alternately, instead of an **allow list** *that enumerates which systems or services are in scope, you may choose to use a* **blocklist** *to describe which are out of scope.*

Please ensure that you have authority to authorize security testing on the systems or services to be included. Specifically, if you engage vendors (e.g., have a managed service provider or use software as a service), confirm whether the third party has explicitly authorized such testing, such as in your agency's contract with the provider or a publicly available policy of the provider. If not, you should work with the vendor to obtain authorization. If it is not possible to obtain the vendor's authorization, you will need to scope those systems or services out of your policy.

Note:

- *After your policy's publication, newly created Internet-accessible systems or services should be included* implicitly *in the scope (e.g., by indicating a wildcard [*] on a domain's scope) or* explicitly *by updating the policy to account for these systems.*
- *As noted above, if you are unable to obtain authorization for specific systems or services supplied by third parties, then you should exclude them from testing under your VDP. However, you should aim to include within your policy's scope all internet-accessible systems or services used by your agency, as they may present risk to your agency even if hosted or provided by third parties.*

This policy applies to the following systems and services:

- *.agency-brand.gov
- agency-form.gov
- agency-service.gov, and the following hostnames:
  - alpaca.agency-service.gov
  - buffalo.agency-service.gov
  - cassowary.agency-service.gov
  - dormouse.agency-service.gov
  - Any other subdomain of agency-service.gov and all customer applications are excluded from this policy (*.app.agency-service.gov is specifically excluded, except for *.service-proxy.app.agency-service.gov.)

- Source code at https://github.com/agency-example/repo

Any service not expressly listed above, such as any connected services (i.e. cloud or software as a service services), are excluded from scope and are not authorized for testing. Additionally, vulnerabilities found in non-ENTITY NAME 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 aren't sure whether a system or endpoint is in scope or not, contact us at changeme@entity.gov before starting your research or at the security contact for the system's domain name listed in the .gov WHOIS

Though we develop and maintain other internet-accessible systems or services, we ask that *active research and testing* only be conducted on the systems and services covered by the scope of this document. If there is a particular system not in scope that you think merits testing, please contact us to discuss it first. We may increase the scope of this policy over time.

Types of testing

The following test types are not authorized:

- Network denial of service (DoS or DDoS) tests or other tests that impair access to or damage a system or data.
- Physical testing (e.g. office access, open doors, tailgating), social engineering (e.g. phishing, vishing), or any other non-technical vulnerability testing.

Reporting a vulnerability

This section describes communication mechanisms and processes for submitting vulnerabilities. It should include instructions on where reports should be sent (e.g., a web form, email address), a request for the information your entity needs to find and analyze the vulnerability (e.g., a description of the vulnerability, its location and potential impact; technical information needed to reproduce; any proof of concept code; etc.). Reporters should be allowed to submit a report anonymously: you should not require the submission of personally identifiable information, although you might request the reporter voluntarily provide contact information.

This is also a good place to pledge your entity to be as transparent as possible about what steps you are taking during the remediation process, as well as set expectations for when the reporter can anticipate acknowledgement of their report.

Information submitted under this policy will be used only to mitigate or remediate vulnerabilities.

We accept vulnerability reports via changeme@agency.gov or at this form**.** Reports may be submitted anonymously.

We will acknowledge receipt of your report within 3 business days.

Please find our PGP encryption key for emails HERE.

PGP encryption keys are easy to use; we recommend them as a primary way of communicating with researchers. If you choose to use a secure web form, make sure it has a strong HTTPS configuration.

SAMPLE

What we would like to see from you

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

- Describe the vulnerability, where it 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.

Please keep your vulnerability reports current by sending us any new information as it becomes available.

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 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.

Document change history

Version	Date	Description
1.0	*Month Day, Year*	First issuance.