Network Vulnerability Assessment and Penetration Testing

For

National Archives and Records Administration (NARA)

Under Contract # GS-23F-0135L

October 18, 2010

By

Clifton Gunderson LLP
Certified Public Accountants & Consultants

TABLE OF CONTENTS

PAGE

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Paul Brachfeld
Inspector General
National Archives and Records Administration
8601 Adelphi Road
College Park, MD 20740-6001

Dear Mr. Brachfeld,

We have completed our vulnerability assessment and penetration testing of National Archives and Records Administration's (NARA) internal and external network infrastructure and environment. The purpose of this testing is to assist NARA in the protection of its IT infrastructure, environment, and digital assets. Our testing results and findings are contained in the enclosed report.

The report contains sensitive and confidential information. Recipients of this report must not, under any circumstances, show or release its contents for purposes other than official review. It must be safeguarded to prevent publication or other improper disclosure of the information it contains. Distribution of this report should be on a need to know basis.

We appreciate your confidence in us to perform these tasks. Should you require additional information, please contact George Fallon at 301-931-2050 or George.Fallon@cliftoncpa.com.

Sincerely,

CLIFTON GUNDERSON LLP

Clifton Gunderson LLP

October 18, 2010
Calverton, Maryland

11710 Beltsville Drive, Suite 300
Calverton, MD 20705-3106
tel: 301-931-2050
fax: 301-931-1710

www.cliftoncpa.com

Executive Summary

NARA contracted with Clifton Gunderson, LLP (CG) to perform external and internal network and penetration testing of the NARA computer network systems in order to assess the chances that an intruder could intentionally or accidentally gain access to NARA's network or systems.

Our testing focused upon
, used to support NARA at

Our assessment included the network mapping of the target systems, scanning of NARA's network infrastructure for weaknesses or flaws (i.e. vulnerabilities), which can allow an attacker to compromise the network by circumventing NARA's administrative and security controls. We then attempted to exploit these system vulnerabilities to gain unauthorized access, including the escalation of system privileges in order to attack other systems within the trusted environment.

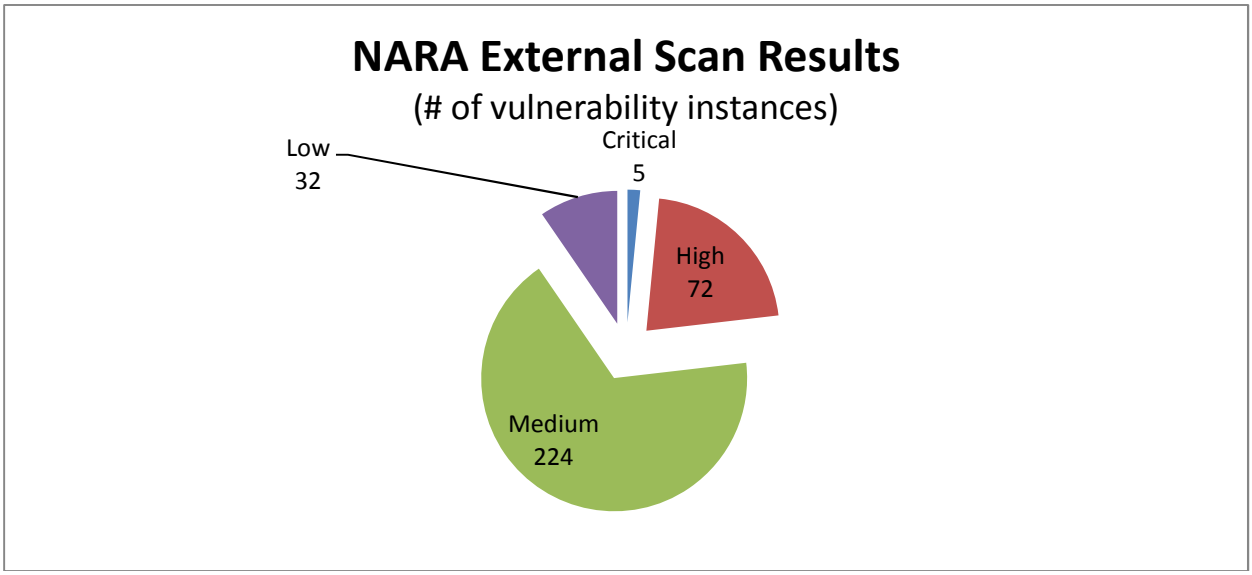
We performed these scans from inside and outside of NARA's firewall to simulate attacks from an external intruder (zero knowledge), an internal employee, and an individual from a University Network attached to NARANet.

During our scans, we gathered sensitive information about NARA's network. We collected information about NARA's network servers, workstations, routers and other network devices. We also analyzed the operating systems versions and patch levels, ports or services running on NARA's network devices.

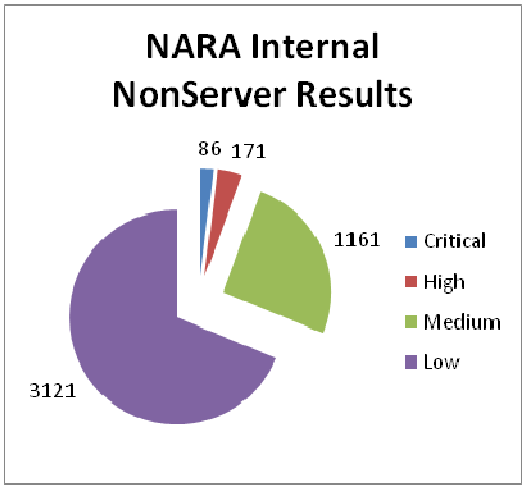
The purpose of this assessment is to assist NARA in the protection of its IT infrastructure, environment, and digital assets. This assessment will help determine the effectiveness of NARA's information systems security in preventing and detecting unauthorized external and internal access to logical assets, and provides a snapshot evaluation of NARA's security posture and potential vulnerabilities that should be remediated. As is the case with a dynamic environment subject to constant change, any projection of the assessment results to the future is subject to the risk that because of change, the results may no longer portray the security posture of the IT infrastructure and environment. Furthermore, the projection of any conclusions, based on our findings to future periods is subject to the risk that changes made to the IT infrastructure and environment may alter the validity of such conclusions.

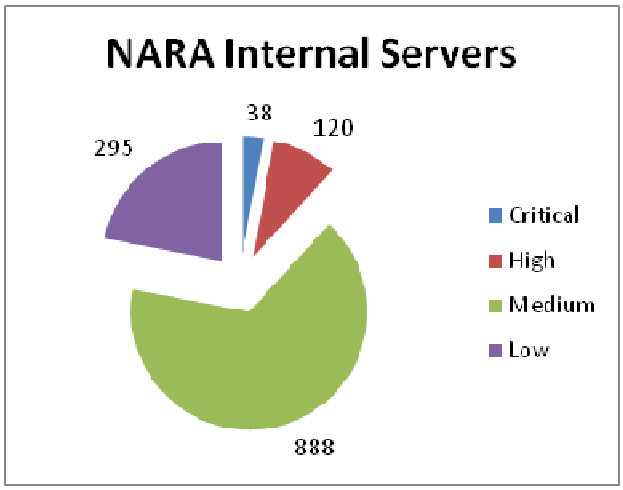
We identified several improvements to be made to the configuration, upgrade and patch management processes of various external and internal facing networks and infrastructure devices. Scan results are categorized by severity ratings as either "Critical," "High," Medium" or "Low." A "critical" or "high" vulnerability is likely if exploited to provide complete remote access to the target system. A "medium" vulnerability generally provides network access if located on the same subnet. A "low" vulnerability requires physical access to the system or requires a command prompt to the system to exploit.

In summary, as a result of our external scan analysis, we noted 333 vulnerability instances comprised of (5) Critical, (72) High, (224) Medium and (32) Low risk, some of which could be exploited by an intruder to intentionally or accidentally gain access to NARA's network or systems. Details are graphically portrayed below:



As a result of our internal scan analysis, we noted a total of 5,880 vulnerability instances, (identified as server and non-server weaknesses) comprised of (124) Critical, (291) High, (2,049) Medium and (3,416) Low, some of which could be exploited by an intruder to intentionally or accidentally gain access to NARA's network or systems. Details are graphically portrayed below:





We made fourteen recommendations which are detailed within the Finding and Recommendation section below.

Objectives, Scope and Methodology

The overall objective was to perform external and internal network and penetration testing of the NARA computer network systems in order to assess the chances that an intruder could intentionally or accidentally gain access to NARA's network or systems.

To accomplish our objective, testing was conducted over the External and Internal network and both sets of tests consisted of four phases:

- Discovery (information gathering),
- Vulnerability Analysis,
- Exploitation and
- Reporting

During the discovery phase, we attempted to obtain information about NARA's network. To obtain this information, we used public sources for external testing and network identification. First, we tested for information available on the internet that is not under NARA's control. We gathered information that is publically available about NARA on the internet. We considered searches for attempts at misuse of the NARA's domain name (nara.gov) by non-authorized parties. In addition, we performed searches on public search engines (e.g. Google). Our testing efforts also included the following:

- Social engineering efforts to access network services,
- Sweeps of buildings to locate wireless access points,
- Sweeps of external web servers,
- Applications in common usage including e-mail and database applications,
- Firewalls, routers and intrusion detection systems to include both Host Intrusion and Network intrusion detection systems, and
- Modernization equipment including the infrastructure connectivity.

Secondly, we tested the network assets that are under the control of NARA. We gathered information about NARA's networks and analyzed the information to identify potential vulnerabilities. We identified public services offered through NARA's internet-facing servers. Among these services are Electronic Mail and Web Servers. After our information gathering and analysis, we tested the effectiveness of the protection of these public services and the servers that host these processes. In addition, we identified versions of software and checked for known vulnerabilities. In addition, we tested for programming flaws such that an attacker could use a weakness to perform a series of steps, which could result in a compromise.

Thirdly, to determine whether noted medium to critical ranked vulnerabilities with a high number of noted instances could be exploited, we attempted to compromise these vulnerabilities to take advantage of on related assets.

To perform our social engineering efforts, we were provided with an acceptable use policy and security awareness training material. Throughout the policy, the awareness training includes instruction relating to the analysis of email, reminding the user to monitor the senders email address and warning about visiting websites that are questionable.

During our wireless scanning efforts, the Archives II building was scanned for wireless network access point detection. We implemented a packet capture assessment using the wireless scanning tool to identify wireless access points and any associated clients that have authenticated to the access point. In addition, identified the .

Our approach to performing the network security testing was in accordance with ***NIST SP 800-115*** "*Technical Guide to Information Security Testing and Assessment*", NARA Notice 2010-045, NARA Penalty Guide (Personnel 300 – Appendix 752A), NARA's Media Protection Methodology and other applicable NARA Security Policies. We provided complete details of tests to the Technical Point of Contact (TPOC) and OIG. We announced testing windows but not specific dates and times for testing and reported testing progress to the TPOC and OIG. During our overt testing activity, we monitored NARA's response to our testing and we took no measures to avoid detection. We conducted logical testing from the Internet and from inside the NARA network. We additionally performed social engineering testing to determine if users would open suspicious emails and click on potentially malicious links.

Our work was performed at as well as during September 2010. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Findings and Recommendations

After we performed our scanning, we analyzed the results to validate potential vulnerabilities found during the discovery phase. We found the following vulnerabilities that a hacker could exploit to potentially compromise NARA's network, and in several cases actually exploit to obtain unauthorized access or escalation of user privileges:

Finding #1

Out of date software patches on several servers permit , and the ability to .

During internal network vulnerability scanning, we noted several remote network hosts running versions of software such as which are vulnerable to

Upon attempting to exploit those servers with , CG was able to compromise two machines, resulting in complete system level access, which was not detected.

Note: Details of the affected machines with Internet Protocol (IP) addresses were provided to (Office of Information Services) NH and the OIG within a separate document (spreadsheet, entitled "NARA Analysis.xls") due to the sensitivity of this data.

Criteria:

- **National Institute of Standards and Technology Special Publication 800-53, revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009**

  SI-2 FLAW REMEDIATION
  Control: The organization:
  a. Identifies, reports, and corrects information system flaws;
  b. Tests software updates related to flaw remediation for effectiveness and potential side effects on organizational information systems before installation; and
  c. Incorporates flaw remediation into the organizational configuration management process.

  Supplemental Guidance: The organization identifies information systems containing software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws) and reports this information to designated organizational officials with information security responsibilities (e.g., senior information security officers, information system security managers, information systems security officers). The organization (including any contractor to the organization) promptly installs security-relevant software updates (e.g., patches, service packs, and hot fixes). Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling, are also addressed expeditiously. Organizations are encouraged to use resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered

in organizational information systems. By requiring that flaw remediation be incorporated into the organizational configuration management process, it is the intent of this control that required/anticipated remediation actions are tracked and verified. An example of expected flaw remediation that would be so verified is whether the procedures contained in USCERT guidance and Information Assurance Vulnerability Alerts have been accomplished. Related controls: CA-2, CA-7, CM-3, MA-2, IR-4, RA-5, SA-11, SI-11.

Control Enhancements:

(1) The organization centrally manages the flaw remediation process and installs software updates automatically.

Enhancement Supplemental Guidance: Due to information system integrity and availability concerns, organizations give careful consideration to the methodology used to carry out automatic updates.

(2) The organization employs automated mechanisms [*Assignment: organization-defined frequency*] to determine the state of information system components with regard to flaw remediation.

(3) The organization measures the time between flaw identification and flaw remediation, comparing with [*Assignment: organization-defined benchmarks*].

(4) The organization employs automated patch management tools to facilitate flaw remediation to [*Assignment: organization-defined information system components*].

References: NIST Special Publication 800-40.

- **National Institute of Standards and Technology Special Publication 800-40, Version 2, *Creating a Patch and Vulnerability Management Program*, November 2005**

  6. Conclusions and Summary of Major Recommendations

  A summary of the primary recommendations is as follows:

  1. Create a patch and vulnerability group.
  2. Continuously monitor for vulnerabilities, remediation, and threats.
  3. Prioritize patch application and use phased deployments as appropriate.
  4. Test patches prior to deployment.
  5. Deploy enterprise-wide automated patching solutions.
  6. Use automatically updating applications as appropriate.
  7. Create an inventory of all information technology assets.
  8. Use standardized configurations for IT resources as much as possible.

9. Verify that vulnerabilities have been remediated.

10. Consistently measure the effectiveness of the organization's patch and vulnerability management program, and apply corrective actions as necessary.

11. Train applicable staff on vulnerability monitoring and remediation techniques.

12. Periodically test the effectiveness of the organization's patch and vulnerability management program.

13. Use U.S. government vulnerability mitigation resources as appropriate.

Cause:

The current software version in use has not been updated

Effect:

If an attacker is able to create , it could allow the execution of arbitrary code on this host to take complete control of the affected system or to .

Recommendation:

We recommend NARA management apply the appropriate hot fix referenced in the vendor advisory on the affected machines.

Finding #2

Several weaknesses were noted related to outdated software

A summary of vulnerabilities noted were as follows:

- A server is utilizing an that is affected by multiple flaws and vulnerabilities,
- are for or are
- The is no longer supported by its vendor, and
- Various weaknesses related to execution of code vulnerability were noted.
- Additionally, a server was prone to attacks.

During our external Public-facing asset testing, a website processing military records requests was noted to employ a component with known vulnerabilities. CG was able to perform and gain access to activated user information.

Note: Details of the affected machines with Internet Protocol (IP) addresses were provided to NH and the OIG within a separate document (spreadsheet, entitled "NARA Analysis.xls") due to the sensitivity of this data.

Criteria:

- **National Institute of Standards and Technology Special Publication 800-53, revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009**

  SI-2 FLAW REMEDIATION
  Control: The organization:
  d. Identifies, reports, and corrects information system flaws;
  e. Tests software updates related to flaw remediation for effectiveness and potential side effects on organizational information systems before installation; and
  f. Incorporates flaw remediation into the organizational configuration management process.

  Supplemental Guidance: The organization identifies information systems containing software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws) and reports this information to designated organizational officials with information security responsibilities (e.g., senior information security officers, information system security managers, information systems security officers). The organization (including any contractor to the organization) promptly installs security-relevant software updates (e.g., patches, service packs, and hot fixes). Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling, are also addressed expeditiously. Organizations are encouraged to use resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in organizational information systems. By requiring that flaw remediation be incorporated into the organizational configuration management process, it is the intent of this control that required/anticipated remediation actions are tracked and verified. An example of expected flaw remediation that would be so verified is whether the procedures contained in USCERT guidance and Information Assurance Vulnerability Alerts have been accomplished. Related controls: CA-2, CA-7, CM-3, MA-2, IR-4, RA-5, SA-11, SI-11.

  Control Enhancements:

  (1) The organization centrally manages the flaw remediation process and installs software updates automatically.

  Enhancement Supplemental Guidance: Due to information system integrity and availability concerns, organizations give careful consideration to the methodology used to carry out automatic updates.

  (2) The organization employs automated mechanisms [*Assignment: organization-defined frequency*] to determine the state of information system components with regard to flaw remediation.

  (3) The organization measures the time between flaw identification and flaw remediation, comparing with [*Assignment: organization-defined benchmarks*].

  (4) The organization employs automated patch management tools to facilitate flaw remediation to [*Assignment: organization-defined information system components*].

References: NIST Special Publication 800-40.

- **National Institute of Standards and Technology Special Publication 800-40, Version 2, *Creating a Patch and Vulnerability Management Program*, November 2005**

  6. Conclusions and Summary of Major Recommendations

  A summary of the primary recommendations is as follows:

  1. Create a patch and vulnerability group.
  2. Continuously monitor for vulnerabilities, remediation, and threats.
  3. Prioritize patch application and use phased deployments as appropriate.
  4. Test patches prior to deployment.
  5. Deploy enterprise-wide automated patching solutions.
  6. Use automatically updating applications as appropriate.
  7. Create an inventory of all information technology assets.
  8. Use standardized configurations for IT resources as much as possible.
  9. Verify that vulnerabilities have been remediated.
  10. Consistently measure the effectiveness of the organization's patch and vulnerability management program, and apply corrective actions as necessary.
  11. Train applicable staff on vulnerability monitoring and remediation techniques.
  12. Periodically test the effectiveness of the organization's patch and vulnerability management program.
  13. Use U.S. government vulnerability mitigation resources as appropriate.

Cause:

The current process to maintain [redacted] is not working effectively.

Effects:

- The [redacted] could be exploited to perform attacks, insert arbitrary plaintext by [redacted], enable , denial of service, or bypass [redacted]
- For the unsupported [redacted] system, this means that no new security patches will be provided [redacted] whom is also unlikely to investigate or acknowledge reports of vulnerabilities in it.

- If a is running a web server that fails to adequately an attack may be able to cause arbitrary and to be executed in a users' browser within the security context of the affected site.

Recommendations:

We recommend NARA management implement the following corrective actions on the affected machines: 1) Upgrade to 2) purchase or generate new , 3) upgrade to a different version of supported by its vendor, and 4) contact the vendor for a patch or upgrade to the

Finding #3

Several network security configuration weaknesses were noted.

Vulnerabilities identified which are categorized as configuration weaknesses are listed below:

- It is possible to access with root privileges,
- Various weaknesses were identified related to

  and
- services support the use of weak .
- The is not password protected.

Upon attempting to exploit the vulnerability, we were able to access Oracle database instances on two machines which were configured with The resulting compromise provided read access into system level databases to include the users database. A listing of all users was possible. This testing concluded with no immediate responsive actions. If time were to permit, the ability to compromise using could lead to unauthorized access.

Additionally, we were able to gain access to several . Based upon the permissions gained, unauthorized configuration changes could be applied to those In addition, software was available to allow the unauthenticated user access to documents

Note: Details of the affected with Internet Protocol (IP) addresses were provided to NH and the OIG within a separate document (spreadsheet, entitled "NARA Analysis.xls") due to the sensitivity of this data.

Criteria:

- **National Institute of Standards and Technology Special Publication 800-53, revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009**

SI-2 FLAW REMEDIATION

Control: The organization:

g. Identifies, reports, and corrects information system flaws;
h. Tests software updates related to flaw remediation for effectiveness and potential side effects on organizational information systems before installation; and
i. Incorporates flaw remediation into the organizational configuration management process.

Supplemental Guidance: The organization identifies information systems containing software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws) and reports this information to designated organizational officials with information security responsibilities (e.g., senior information security officers, information system security managers, information systems security officers). The organization (including any contractor to the organization) promptly installs security-relevant software updates (e.g., patches, service packs, and hot fixes). Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling, are also addressed expeditiously. Organizations are encouraged to use resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in organizational information systems. By requiring that flaw remediation be incorporated into the organizational configuration management process, it is the intent of this control that required/anticipated remediation actions are tracked and verified. An example of expected flaw remediation that would be so verified is whether the procedures contained in USCERT guidance and Information Assurance Vulnerability Alerts have been accomplished. Related controls: CA-2, CA-7, CM-3, MA-2, IR-4, RA-5, SA-11, SI-11.

Control Enhancements:

(1) The organization centrally manages the flaw remediation process and installs software updates automatically.

Enhancement Supplemental Guidance: Due to information system integrity and availability concerns, organizations give careful consideration to the methodology used to carry out automatic updates.

(2) The organization employs automated mechanisms [*Assignment: organization-defined frequency*] to determine the state of information system components with regard to flaw remediation.

(3) The organization measures the time between flaw identification and flaw remediation, comparing with [*Assignment: organization-defined benchmarks*].

(4) The organization employs automated patch management tools to facilitate flaw remediation to [*Assignment: organization-defined information system components*].

References: NIST Special Publication 800-40.

- **National Institute of Standards and Technology Special Publication 800-40, Version 2, *Creating a Patch and Vulnerability Management Program*, November 2005**

6. Conclusions and Summary of Major Recommendations

A summary of the primary recommendations is as follows:

1. Create a patch and vulnerability group.
2. Continuously monitor for vulnerabilities, remediations, and threats.
3. Prioritize patch application and use phased deployments as appropriate.
4. Test patches prior to deployment.
5. Deploy enterprise-wide automated patching solutions.
6. Use automatically updating applications as appropriate.
7. Create an inventory of all information technology assets.
8. Use standardized configurations for IT resources as much as possible.
9. Verify that vulnerabilities have been remediated.
10. Consistently measure the effectiveness of the organization's patch and vulnerability management program, and apply corrective actions as necessary.
11. Train applicable staff on vulnerability monitoring and remediation techniques.
12. Periodically test the effectiveness of the organization's patch and vulnerability management program.
13. Use U.S. government vulnerability mitigation resources as appropriate.

Cause:

These vulnerabilities were due to the deployment of and deployment of improperly .

Effects:

- If exported by the can be an attacker may be able to leverage this to read (and possibly write) files on
- The weakness on the could allow an attacker to use this computer as a In addition, this type of can be used to create a denial of service condition .
- The provides an attacker information such as how often the system is being used, the names of the users, and more.
- If the accepts connections with weak and attacked may be able to conduct between the affected service and clients.

- If is assigned to the an attacker may use this fact to shut it down arbitrarily, thus preventing legitimate users from using it.

Recommendations:

We recommend NARA management implement the following corrective actions on the affected machines: 1) on the remote host so that only authorized hosts can 2) disable the or upgrade to a more secure one, 3) consult the application's documentation to disable 4) disable the service if not needed, and 5) use the c to assign

Finding #4

An Internet connection was identified which does not follow the same filtering and acceptable use policy as other NARANet Internet connections.

Based upon our review of connectivity and the configuration of the NARANet into the we noted that network traffic flows only outbound from NARA. This network connection is not direct and involves several intervening networks which belong to . We determined that this internet connection is provided through does not follow the same filtering and acceptable use policy as the rest of the NARA network, but could permit NARA users the ability to access Internet sites which are normally restricted by NARA's web filters and potentially out of compliance with NARA's acceptable use policy.

Criteria:

- **National Institute of Standards and Technology Special Publication 800-53, revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009**

  SI-3 MALICIOUS CODE PROTECTION
  Control: The organization:
  a. Employs malicious code protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code:
     - Transported by electronic mail, electronic mail attachments, web accesses, removable
     - Media, or other common means; or
     - Inserted through the exploitation of information system vulnerabilities;
  b. Updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures;
  c. Configures malicious code protection mechanisms to:
     - Perform periodic scans of the information system [Assignment: organization-defined frequency] and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy; and

- Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator; [Assignment: organization-defined action]] in response to malicious code detection; and

d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

Supplemental Guidance: Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, and remote-access servers. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode) or contained within a compressed file. Removable media includes, for example, USB devices, diskettes, or compact disks. A variety of technologies and methods exist to limit or eliminate the effects of malicious code attacks. Pervasive configuration management and strong software integrity controls may be effective in circumventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber attacks that could affect organizational missions and business functions. Traditional malicious code protection mechanisms are not built to detect such code. In these situations, organizations must rely instead on other risk mitigation measures to include, for example, secure coding practices, trusted procurement processes, configuration management and control, and monitoring practices to help ensure that software does not perform functions other than those intended. Related controls: SA-4, SA-8, SA-12, SA-13, SI-4, SI-7.

Control Enhancements:

(1) The organization centrally manages malicious code protection mechanisms.

(2) The information system automatically updates malicious code protection mechanisms (including signature definitions).

(3) The information system prevents non-privileged users from circumventing malicious code protection capabilities.

(4) The information system updates malicious code protection mechanisms only when directed by a privileged user.

(5) The organization does not allow users to introduce removable media into the information system.

(6) The organization tests malicious code protection mechanisms [*Assignment: organization-defined frequency*] by introducing a known benign, non-spreading test case into the information system and subsequently verifying that both detection of the test case and associated incident reporting occur, as required.

References: NIST Special Publication 800-83.

Cause:

Network configuration standards for Internet connectivity have not been consistently applied.

Effect:

This weakness could permit NARA users the ability to access Internet sites with inappropriate content.

Recommendation:

We recommend NH management reconfigure the security of this Internet connection to ensure users are required to comply with NARA's acceptable use policy.

Finding #5

Users were noted clicking on potentially malicious links within emails from an unknown suspicious source.

Based upon security awareness training provided to all individuals with a NARANet account, users are instructed not to accept or click on links within emails of unknown or suspicious origin. To test the effectiveness of this particular portion of their training, we sent an email from an unknown external user to 90 haphazardly selected NARA individuals containing a potentially malicious link, and noted a total of 18% of targeted users actually clicked on these links within the 1st 24 hours. This link was connected to an unrecognizable web server with a redirection to yet another web server. If this link actually was malicious, users could have been infected with a variety of viruses or permit the installation of unauthorized or malicious software on their machines. Also, of the total population tested, 5 (of 6 total) users are located [redacted] clicked on the link. Email filtering successfully restricted attempts to perform this test for the first 4 – 6 hours, but then was successful with [redacted]

Criteria:

Per the NARA Information Systems Security and PII Awareness training material, page 29 Threats: Spam

What is it?

Spam is the abuse of e-mail messaging systems by sending unsolicited bulk messages indiscriminately. Most spam e-mails tend to promote a commercial service or product. Spam is also known as junk e-mail.

How can it harm?

Some spam messages contain viruses or links to malicious websites. Spam can also be used to cause denial of service attacks.

What can I do?

Delete the e-mail without opening it.

Cause:

Users are not following the NARA security awareness training requirement to ensure the safety and security of the NARANet and NARA systems and data in regards to email usage.

Effect:

As users were directed to a malicious site this could have infected/compromised their computer with a variety of viruses or permit the installation of unauthorized or malicious software on their machines, which could be used as a launching point to infect/compromise other computers within the NARA network.

Recommendation:

We recommend NARA management reinforce the component related to email usage in their security awareness training material provided to NARA system users.

Finding #6

Our internal and external NARA network vulnerability assessments identified a large number of vulnerabilities, including many designated "critical" and "high."

As a result of our vulnerability assessment of the NARA network during September 2010, we noted a total of 5,880 vulnerability instances, comprised of 124 Critical, 291 High, 2,049 Medium and 3,416 Low. The "critical" vulnerability instances represent 12 unique vulnerabilities as follows:

- External Network
  - [redacted] are no longer supported by the Vendor
- Internal Network
  - An unpatched flaw in the [redacted].
  - An unpatched flaw in the [redacted].
  - An unpatched flaw in the [redacted].
  - It is possible to bypass authentication with
  - An [redacted] allows execution of arbitrary code.
  - The [redacted] has a backdoor.
  - An unpatched application that is affected by a
  - The [redacted] is not supported by its vendor any more.
  - The [redacted] uses default credentials.
  - [redacted] have multiple vulnerabilities resulting in .
  - The [redacted] is protected using a known set of credentials.

The "high" vulnerability instances represent 15 unique vulnerabilities as follows:

- External Network
  - [redacted] is running on the server.
    - This finding resulted from the [redacted]

  - o using outdated versions of affected by multiple flaws.
- Internal Network
  - o An unpatched flaw in
  - o An unpatched flaw in
  - o Multiple are available without having root privileges.
  - o The can be guessed.
  - o An unpatched is affected by multiple vulnerabilities.
  - o The is vulnerable to a attack.
  - o An unpatched application is affected by a
  - o The has no
  - o The is protected with .
  - o The is vulnerable to memory corruption flaws resulting in denial of service.
  - o The does not allowing undetected password guessing.
  - o The allows unauthenticated access to an .
  - o The is vulnerable to a attack through a vulnerability.

Note: Details of the affected machines with Internet Protocol (IP) addresses were provided to NH and the OIG within a separate document (spreadsheet, entitled "NARA Analysis.xls") due to the sensitivity of this data.

Criteria:

- **National Institute of Standards and Technology Special Publication 800-53, revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009**

  SI-2 FLAW REMEDIATION
  Control: The organization:
  a. Identifies, reports, and corrects information system flaws;
  b. Tests software updates related to flaw remediation for effectiveness and potential side effects on organizational information systems before installation; and
  c. Incorporates flaw remediation into the organizational configuration management process.

  Supplemental Guidance: The organization identifies information systems containing software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws) and reports this information to designated organizational officials with information security responsibilities (e.g., senior information security officers, information system security managers, information systems security officers). The organization (including any contractor to the organization) promptly installs security-relevant software updates (e.g., patches, service packs, and hot fixes). Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling, are also addressed expeditiously. Organizations are encouraged to use resources such as the Common Weakness Enumeration (CWE) or

Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in organizational information systems. By requiring that flaw remediation be incorporated into the organizational configuration management process, it is the intent of this control that required/anticipated remediation actions are tracked and verified. An example of expected flaw remediation that would be so verified is whether the procedures contained in USCERT guidance and Information Assurance Vulnerability Alerts have been accomplished. Related controls: CA-2, CA-7, CM-3, MA-2, IR-4, RA-5, SA-11, SI-11.

Control Enhancements:

(1) The organization centrally manages the flaw remediation process and installs software updates automatically.

Enhancement Supplemental Guidance: Due to information system integrity and availability concerns, organizations give careful consideration to the methodology used to carry out automatic updates.

(2) The organization employs automated mechanisms [*Assignment: organization-defined frequency*] to determine the state of information system components with regard to flaw remediation.

(3) The organization measures the time between flaw identification and flaw remediation, comparing with [*Assignment: organization-defined benchmarks*].

(4) The organization employs automated patch management tools to facilitate flaw remediation to [*Assignment: organization-defined information system components*].

References: NIST Special Publication 800-40.

- **National Institute of Standards and Technology Special Publication 800-40, Version 2, *Creating a Patch and Vulnerability Management Program*, November 2005**

6. Conclusions and Summary of Major Recommendations

A summary of the primary recommendations is as follows:

1. Create a patch and vulnerability group.
2. Continuously monitor for vulnerabilities, remediations, and threats.
3. Prioritize patch application and use phased deployments as appropriate.
4. Test patches prior to deployment.
5. Deploy enterprise-wide automated patching solutions.
6. Use automatically updating applications as appropriate.
7. Create an inventory of all information technology assets.

8. Use standardized configurations for IT resources as much as possible.

9. Verify that vulnerabilities have been remediated.

10. Consistently measure the effectiveness of the organization's patch and vulnerability management program, and apply corrective actions as necessary.

11. Train applicable staff on vulnerability monitoring and remediation techniques.

12. Periodically test the effectiveness of the organization's patch and vulnerability management program.

13. Use U.S. government vulnerability mitigation resources as appropriate.

Cause:

were not applied timely and could have been more secure.

Effect:

If vulnerabilities with a greater potential impact to information systems are exploited, unauthorized individuals could potentially gain inappropriate access to systems and data.

Recommendations:

We recommend NARA management 1) immediately address corrective action for all vulnerabilities identified as "high" and "critical" risk, and 2) evaluate the identified risks and corrective actions to address those identified as "medium" and "low" risk vulnerabilities.