



# United States Department of the Interior

OFFICE OF INSPECTOR GENERAL  
Washington, DC 20240


SEP - 6 2005

## Memorandum

To: P. Lynn Scarlett  
Assistant Secretary - Policy, Management and Budget

James Cason  
Associate Deputy Secretary

W. Hord Tipton  
Chief Information Officer

From: Earl E. Devaney  
Inspector General 

Subject: Penetration Testing

The penetration testing conducted on Information Technology (IT) networks of the Department of the Interior (DOI) by the Office of Inspector General (OIG) through a Memorandum of Understanding (MOU) in 2004 has been completed. This memorandum summarizes our most recent findings, provides a final penetration testing scorecard and an OIG Intrusion Detection Scorecard, and transmits the final technical reports.

Our network security testing consisted of four phases. The first phase, conducted between November 2004 and January 2005, included penetration testing on the United States Geological Survey and the Bureau of Reclamation, and limited testing on the Bureau of Indian Affairs and the Office of the Special Trustee. Phase two, conducted between February and April 2005, included penetration testing on the Bureau of Land Management, the National Business Center, and the Minerals Management Service. Phase three, conducted between May and mid-August 2005, included penetration testing on the Fish and Wildlife Service (FWS), National Park Service (NPS), and the Office of Surface Mining (OSM). We have also completed our IT security evaluation of the Bureau of Reclamation's (BOR) National Critical Infrastructure Information Systems. Phase four will consist of an overall assessment of DOI's IT security, drawing from our work over the past several years, which we intend to publish late this fall.

At the outset of our testing, both the OIG and the Department believed that DOI IT networks were prepared to undergo rigorous testing, given the spate of recently issued policies and guidelines, and the bureaus' and offices' Certification and Accreditation of their IT systems. Unfortunately, as you well know, our testing revealed that several

bureaus and offices still suffer from serious weakness in their security posture. These weaknesses, in turn, negatively impact DOI's IT security overall.

In particular, our penetration testing has demonstrated that DOI's IT network and system architecture have design flaws that create vulnerabilities related to the trusted relationship between systems, networks, and devices. These findings send an important message to all DOI's IT and other senior managers: Inter-connected systems are only as strong as their weakest link. Due to vulnerabilities in several bureaus' IT systems, DOI internal networks, as a whole, are vulnerable to unauthorized access.

On multiple occasions, we found little or no network or application security in use within DOI's internal networks. Remote access vulnerabilities were exploited that allowed our penetration testers to masquerade as authorized users, roam around in the internal networks of some of the most sensitive of DOI systems, and most recently, actually manipulate data.

Rather than simply accepting the results of our testing and promptly addressing the underlying vulnerabilities, the Department and bureaus have, to date, expended considerable time and energy debating our findings, challenging our methodology, and impugning the credentials and integrity of our staff and contractors.

I do not wish to repeat this past experience. Instead, I suggest that we assemble the appropriate Department, bureau and OIG IT professionals charged with conducting a robust review of all vulnerabilities detected and, with the involvement and commitment of the Assistant Secretaries and Bureau Directors, work collectively and cooperatively to make DOI's IT systems more secure. Remediation of identified vulnerabilities should become top priority. Bureaus may consider utilizing the services of an existing contractor to expedite the implementation of solutions.

### **PHASE THREE TEST RESULTS**

In short, the phase 3 test results show that OIG was not able to penetrate FWS and OSM, but that a penetration of NPS allowed testers to traverse to NBC's systems without detection. The findings for phase 3 are summarized below:

#### **Office of Surface Mining**

Penetration testing of the Office of Surface Mining (OSM) noted some vulnerabilities, although none were successfully exploited to gain unauthorized access. The OSM has a small footprint, i.e. few devices open to the internet, and has done a good job of securing their network from intrusion. While no high risk vulnerabilities were detected, we found two instances of vulnerabilities in web applications that OSM should remedy in a timely fashion.

## U.S. Fish and Wildlife Service

The external security posture of FWS did not allow for unauthorized access. By using Intrusion Detection Systems (IDS) and blocking our testing addresses, FWS made it extremely difficult for us to exploit external network based vulnerabilities. However, some medium risk issues and a number of low risk issues were identified. For example, in one instance we were able to access one Intranet web site that provided information on FWS's security policies and employee directories. Intranet web sites should not be accessible from the Internet. We also noted that default web server configuration files were left on some production servers, indicating that the web server was not hardened properly and could be vulnerable to attack. FWS will need to implement the recommendations provided in the accompanying reports.

## National Park Service

Penetration testing of the National Park Service (NPS) systems found the NPS networking infrastructure to be vulnerable to unauthorized access from the Internet. We used this access to gain entry into the NPS Chief Information Officer's internal network and to elevate our access privileges. We carried out our testing activities undetected for nearly a month. Major findings are:

- ❖ Penetrated the [REDACTED] site and created a web page to indicate our control over the server' (See Example 1)
- ❖ Penetrated the [REDACTED] a common web application vulnerability. This allowed us access to tables with many usernames and passwords.
- ❖ Obtained full administrative access to [REDACTED] allowing for administrative access to [REDACTED]
- ❖ Gained access [REDACTED] This was then used to access the [REDACTED]
- ❖ Obtained configurations settings for [REDACTED] (See Example 3)



- ❖ Gained access to [REDACTED]
- ❖ [REDACTED] allowing us to add, modify, and delete records on what appears to be a grants application. (See Example 4)

### Bureau Traversal from NPS Results in Another Compromise of NBC

Having obtained access to the [REDACTED] we conducted bureau traversal testing. We were unable to access [REDACTED] or any of the three offline networks – [REDACTED]. Certain address ranges at [REDACTED] and DOI could be reached, although there were some limitations. For example, addresses in the [REDACTED] could be seen (“pinged”), but actual services, such as [REDACTED]

However, several [REDACTED] servers were reached from within NPS. Accesses to these systems were used to:

- ❖ Gain unauthorized access to servers within the [REDACTED] which had been compromised during previous testing<sup>6</sup>.
- ❖ Obtain user names and passwords for WebFPPS and FPPS<sup>7</sup>.
- ❖ Access the FPPS application with rights to modify and create records and view sensitive privacy and financial information. We made – and then corrected – an address change in FPPS. Having done this, we also believe we could have changed bank routing information and other electronic funds records to potentially divert electronic payments to other banks. (See example 5)

That some of the NBC’s most sensitive personal privacy and financial data have been compromised, yet again, raises grave concerns as to their overall security posture. It is sadly ironic that NBC expended such a considerable effort to refute and diminish our previous penetration success. Based on our ability to successfully traverse from another bureau into the very same sensitive NBC systems suggests that a change in response (and attitude) may be required.

---

<sup>4</sup> A firewall is a device that protects one segment of a network from another by establishing access control lists and permissions. The NPS core firewalls provide the access controls needed to protect NPS from various networks. By obtaining these configurations we could determine what areas to target for further exploitation.

<sup>5</sup> A virtual private network uses the Internet to provide remote users access to the NPS and DOI systems that are usually not intended for public use. Our compromise of the NPS VPN allowed us undetected access to NPS and NBC assets as we were viewed as a trusted NPS user.

<sup>6</sup> See NBC IT Security Penetration Testing-Notice of Potential Findings and Recommendations. April 19, 2005, and NSM-EV-OSS-0025-2005-7-13-05-NBC Penetration Testing External Penetration Testing of National Business Center. July 13, 2005.

<sup>7</sup> These user names and passwords were used to log onto FPPS as a trusted user and allowed us to carry out activities based on the permissions granted to that user. In many instances users had high level of privileges.

## Bureau of Reclamation's National Critical Infrastructure Information Systems

We also carried out IT security reviews at the Bureau of Reclamation's (BOR) dams that have been identified to operate National Critical Infrastructure Information Systems (NCIIS)<sup>8</sup>. These systems are known as Supervisory Control and Data Acquisition (SCADA) which automate many critical functions at the dams. We found that the SCADA systems are operating in relative safety from potentially catastrophic cyber-security threats. This is due principally to BOR's effective implementation of an isolated environment for their NCIIS from public and internal networks.

While this is a good first step in securing some of DOI's most sensitive systems, BOR relies principally on network isolation to secure its NCIIS rather than following best practices for SCADA security. This may provide BOR and the DOI with a false sense of overall security. Our assessment found that these systems remain vulnerable to a malicious insider as the lack of security controls within the NCIIS would allow a determined attacker the potential for service disruption or worse. We noted the following:

- ❖ BOR has not implemented layered security measures, in line with SCADA best practices<sup>9</sup>, such as firewalls and intrusion detection and prevention systems, to fully protect their NCIISs.
- ❖ BOR lacks a technical security assessment program to test the effectiveness of security controls within all National Critical Infrastructure Facilities.
- ❖ BOR does not have processes in place to capture critical workforce knowledge from the impending retirement of skilled staff operating these systems and facilities.
- ❖ BOR lacks a configuration management program and cannot be assured that changes to these critical systems are being implemented correctly and securely.
- ❖ Sensitive SCADA data resides on workstations accessible via the [REDACTED]

We note, however, that BOR is in the process of upgrading some of their aging infrastructure and should be commended for these efforts. We recommend that improved security controls be integrated as a part of these upgrades.

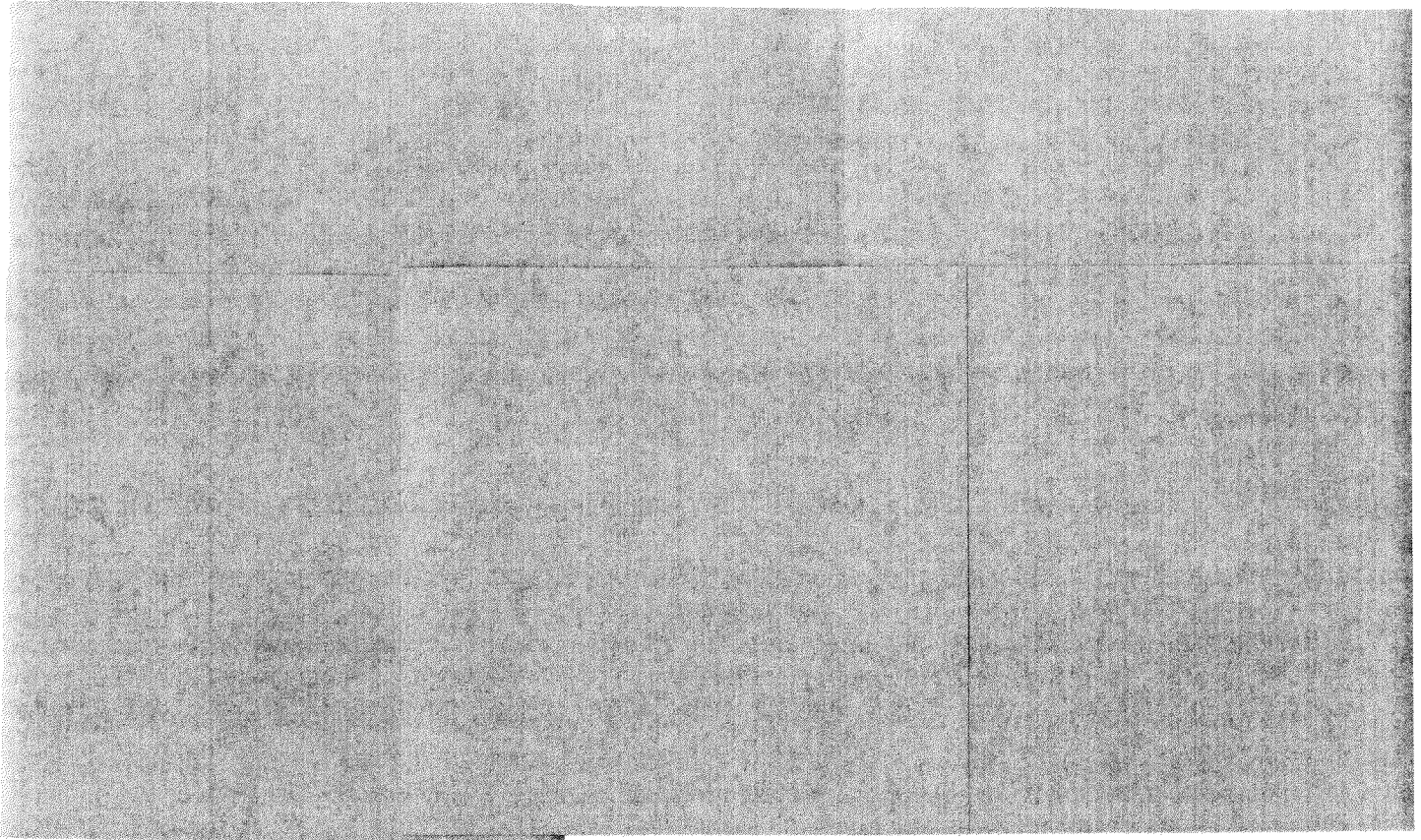
---

<sup>8</sup> Systems that support our nation's critical infrastructures. Critical Infrastructures are "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, page 6. February 2003.

<sup>9</sup> 21 Steps to Improve Cyber Security of SCADA Networks, A Joint Publication of the President's Critical Infrastructure Protection Board and the Department of Energy. September 2002.

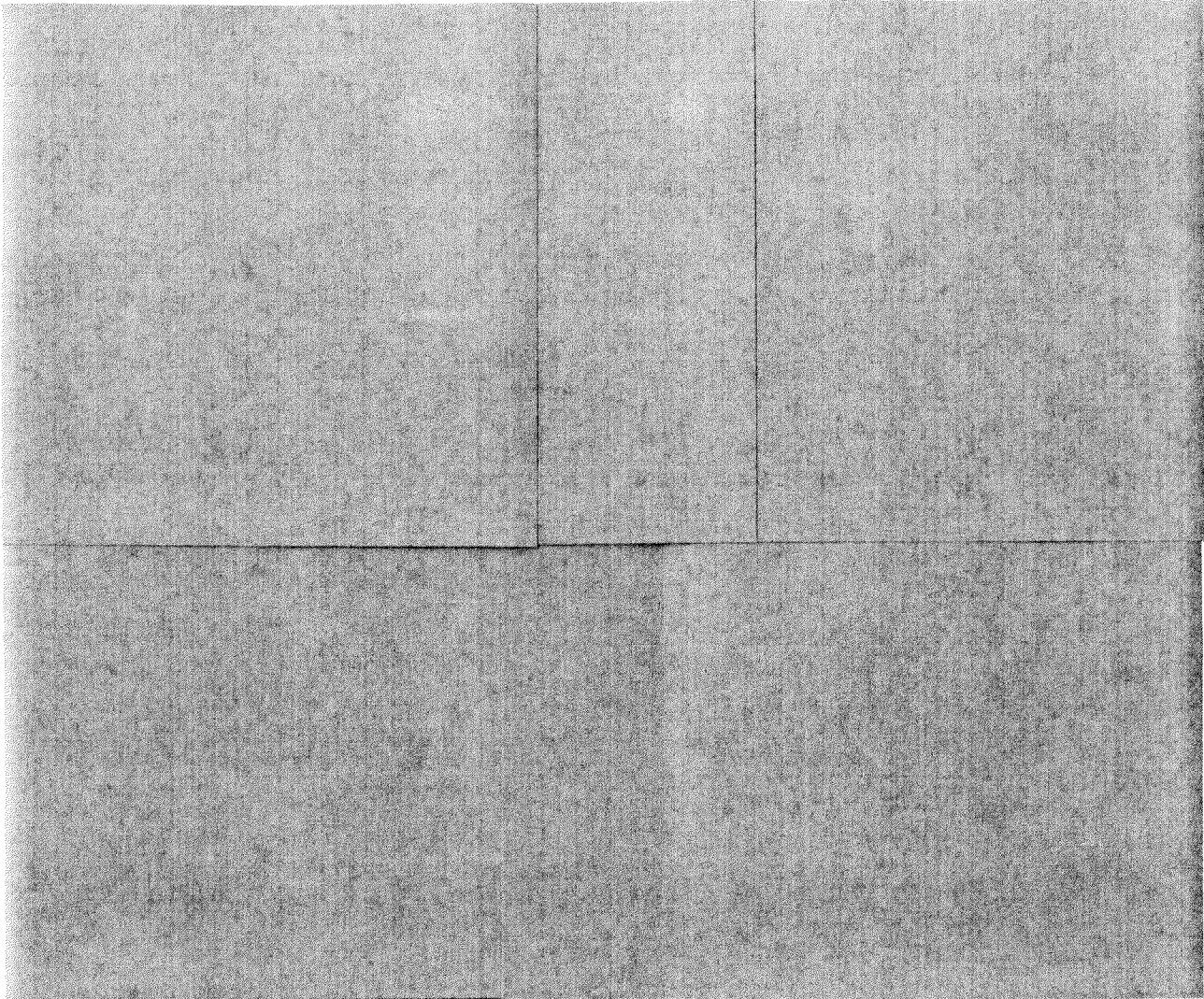
Attachments: Examples 1-5  
Penetration Testing Scorecard  
Intrusion Detection Scorecard  
Technical Reports for OSM, FWS, SCADA

# EXAMPLES

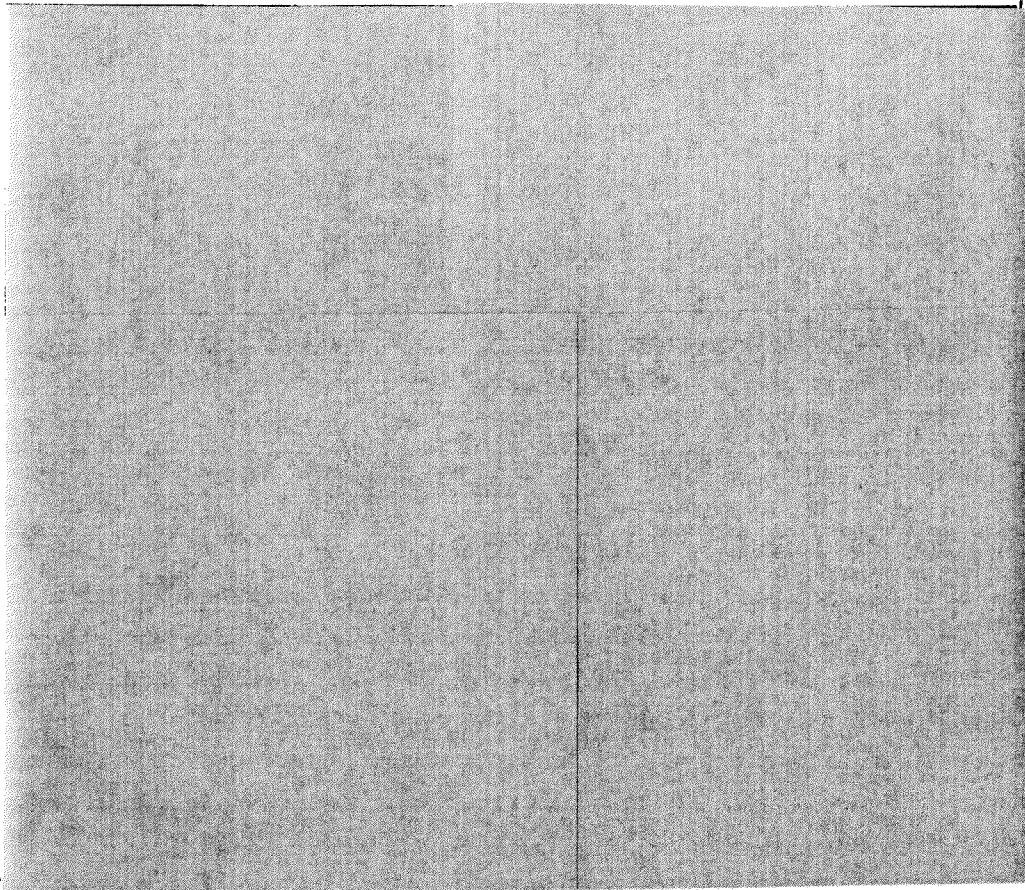


**Example 1. Penetration of [www.recreation.gov](http://www.recreation.gov).**

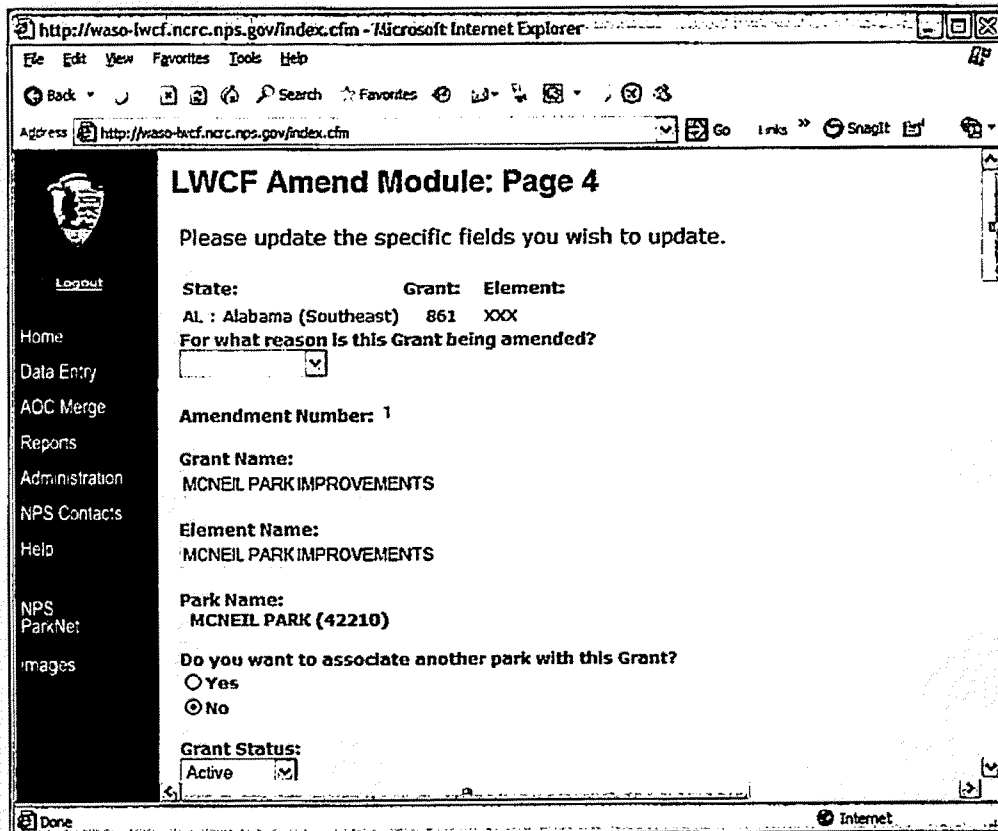




**Example 2. Copy of email sent by the OIG from NPS Director Fran Mainella mail box to OIG staff involved with penetration testing.**



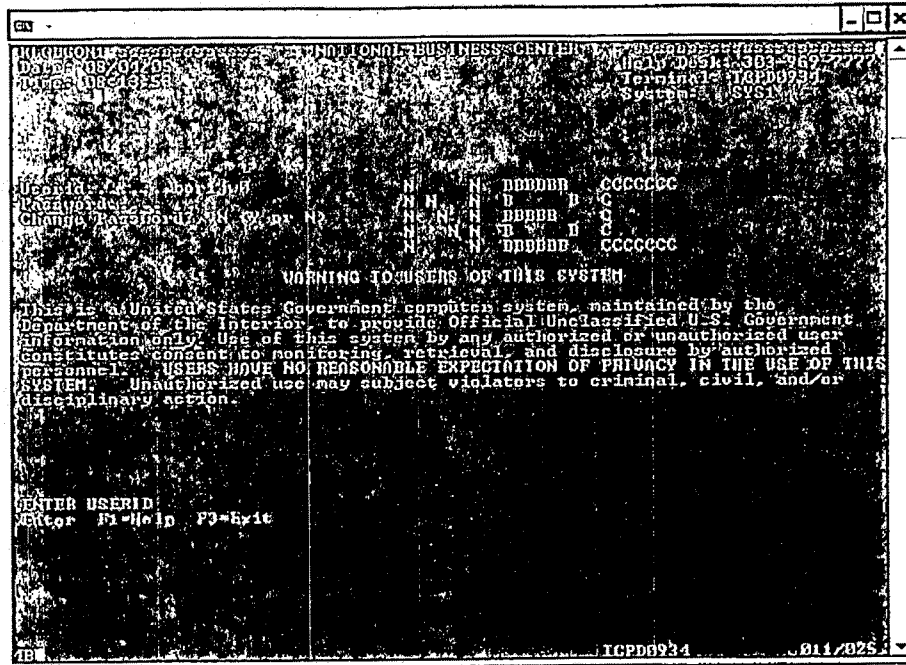
**Example 3. Full configuration files for NPS's main firewalls were obtained.**



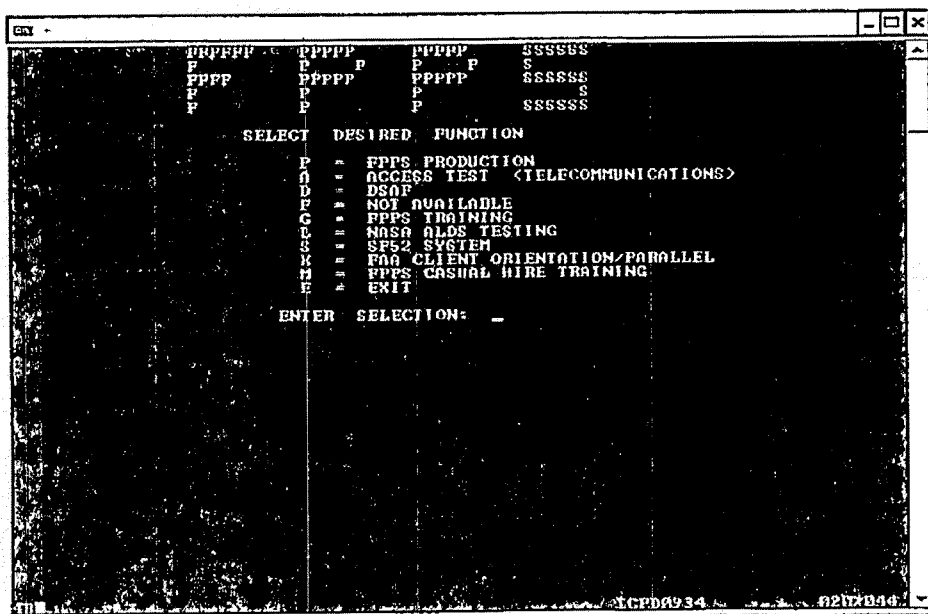
Example 4. Full, unauthorized access to the Land Water Conservation Fund application.

Example 5

Login Screen

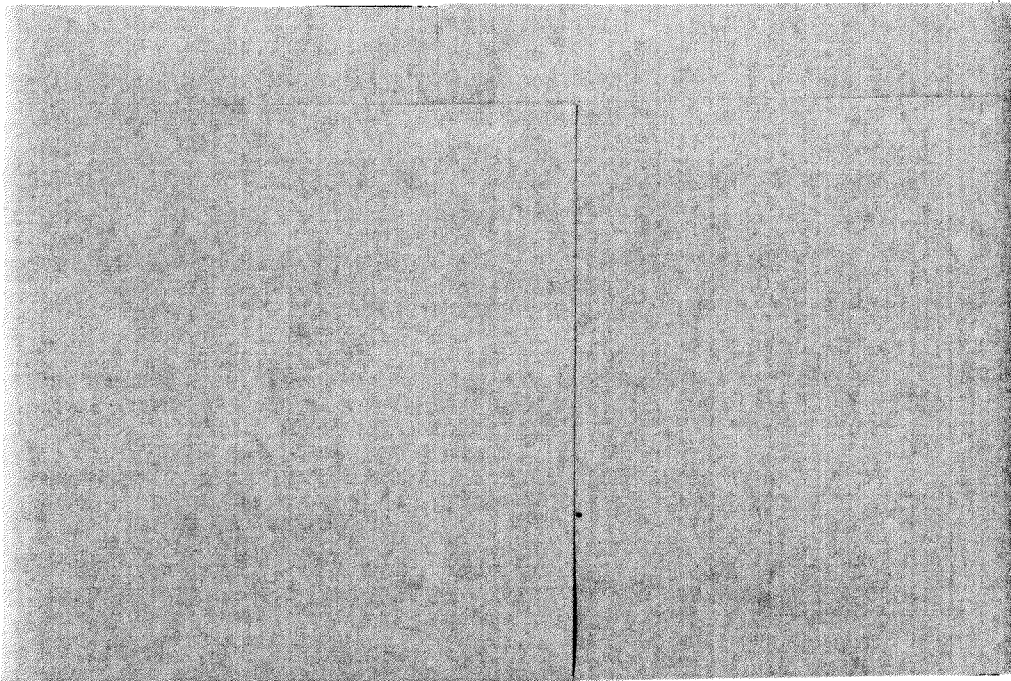


FPPS Main menu

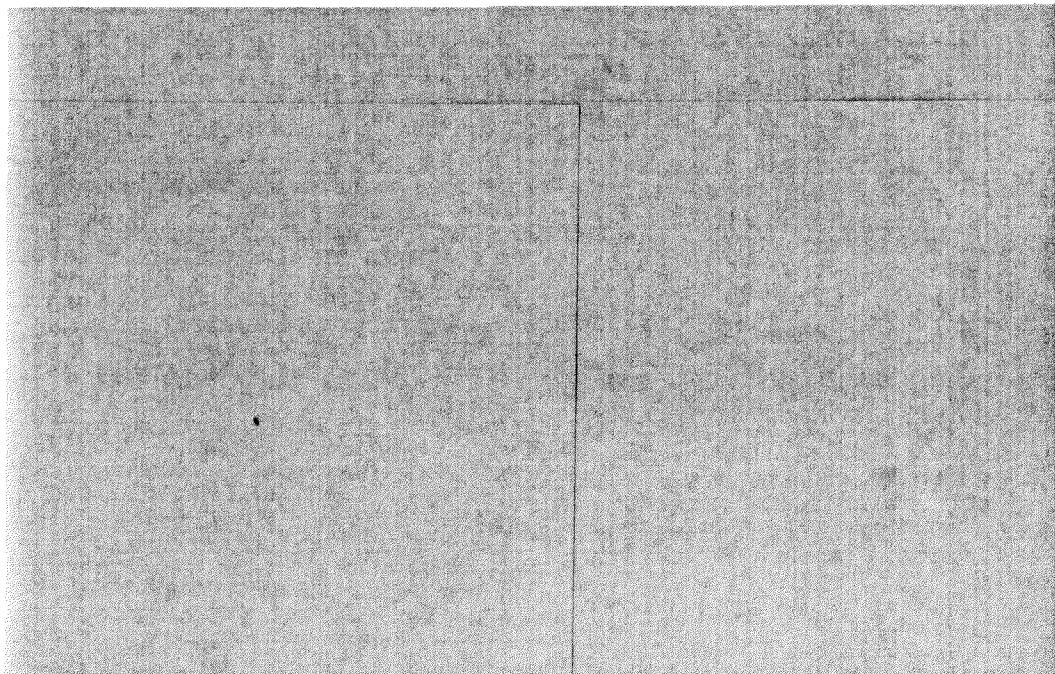




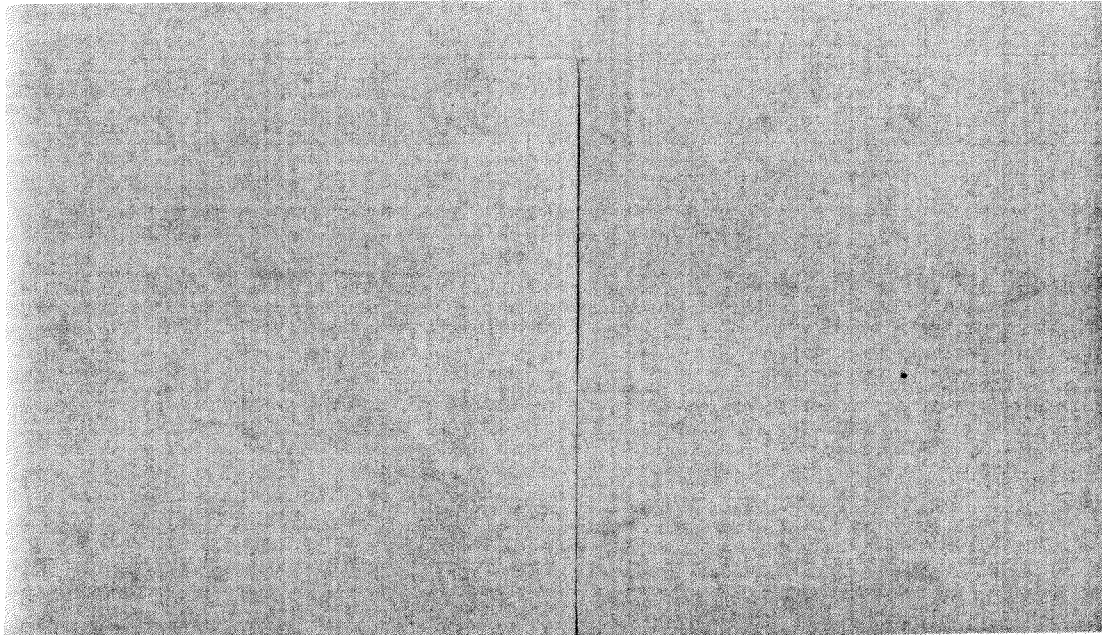
**FPPS Employee Maintenance Screen**



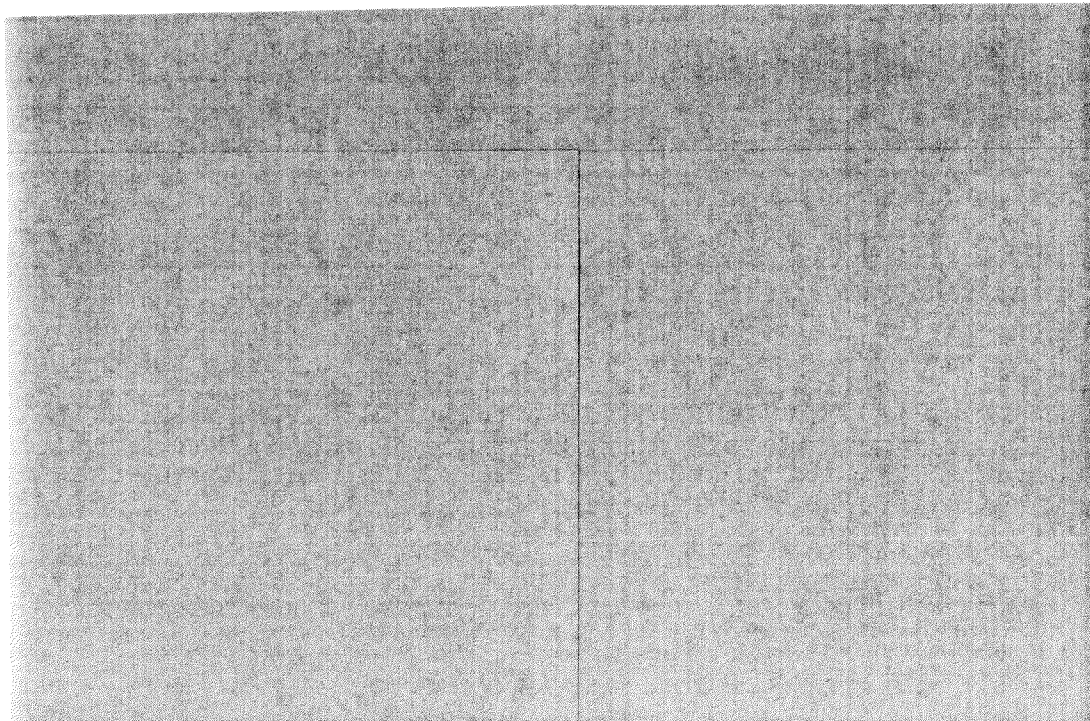
**Social Security Number for BOR Commissioner John Keys**



Initiate Address Change for BOR Commissioner John Keys

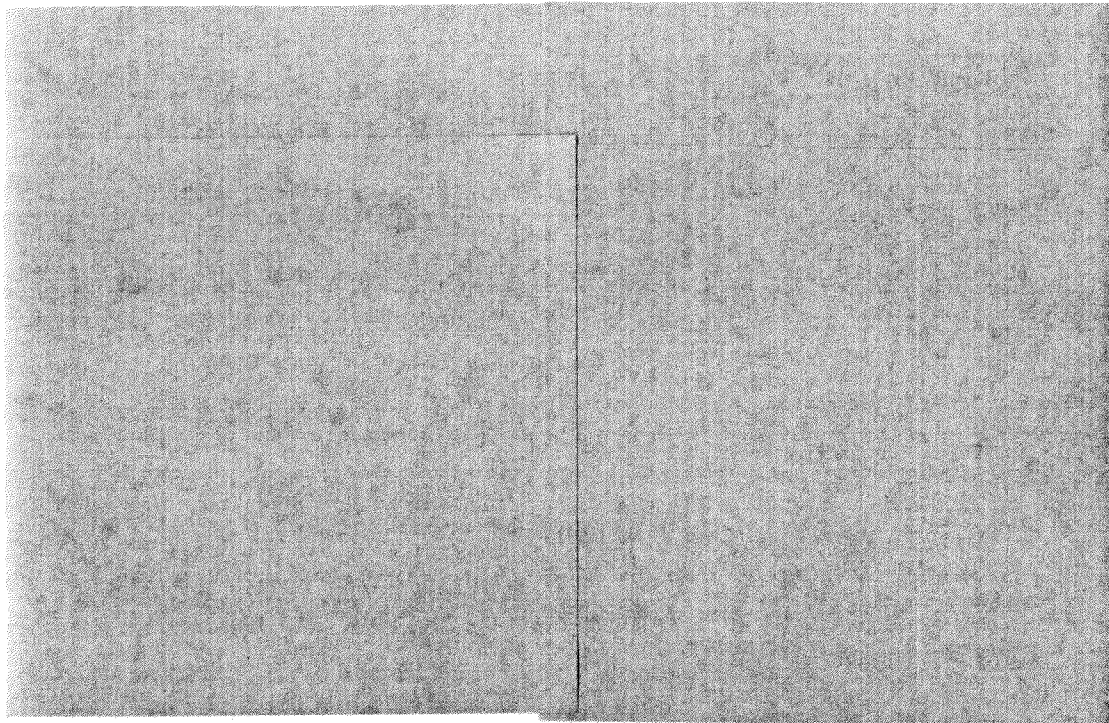


Added XXX At End of Apartment Address for BOR Commissioner John Keys

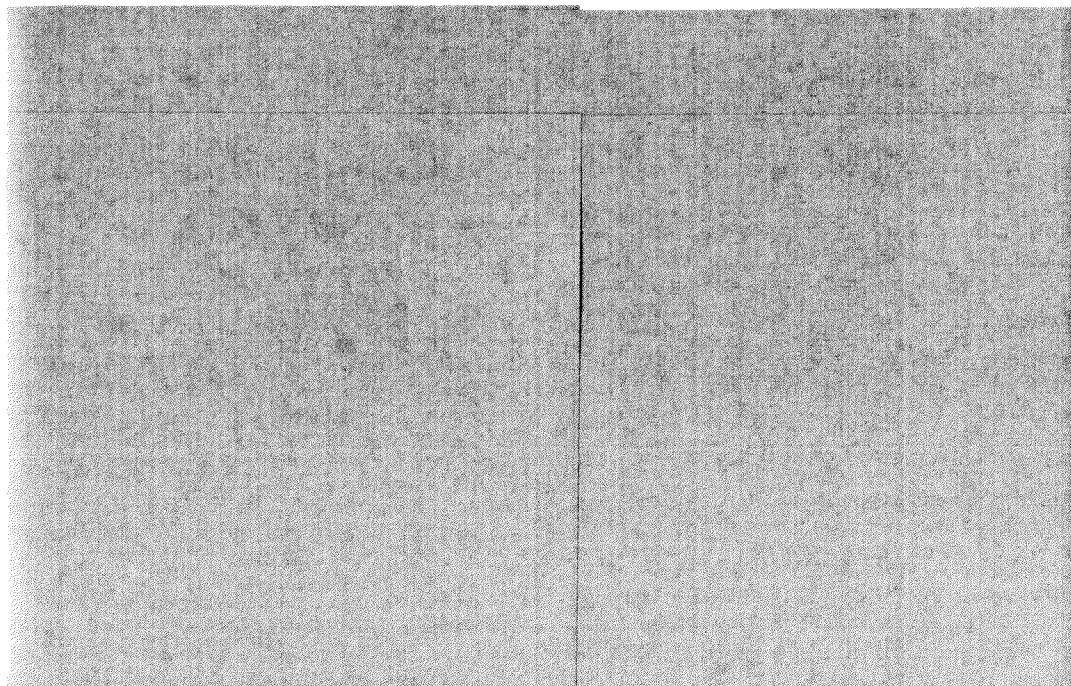




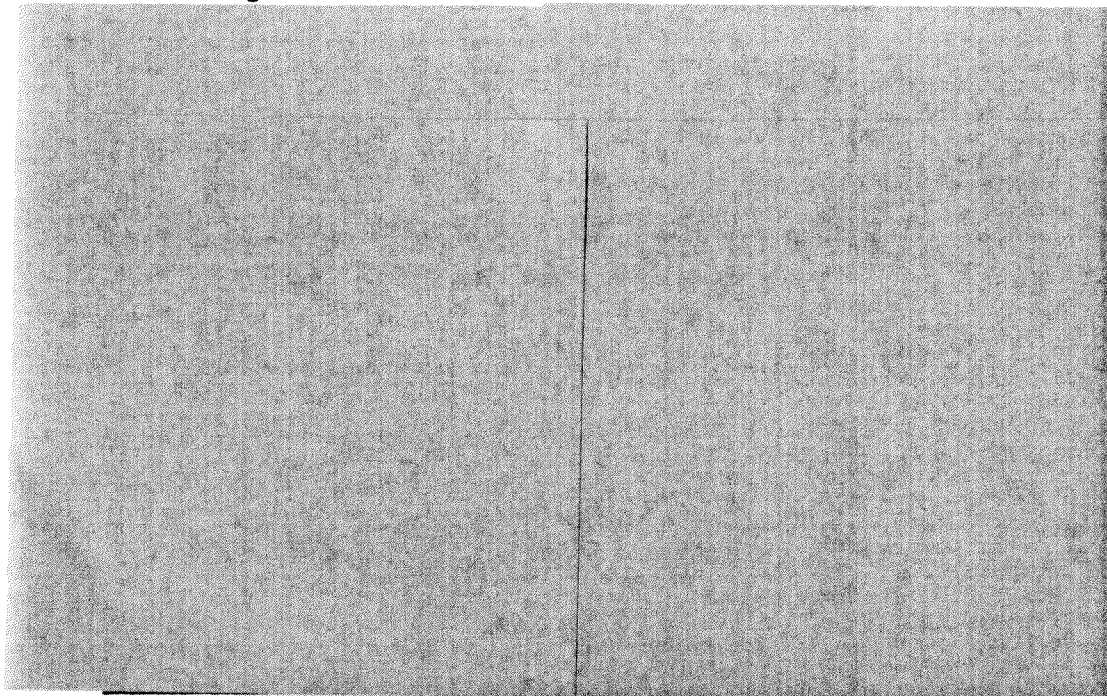
FPPS Accepted Address Change for Apartment [REDACTED]



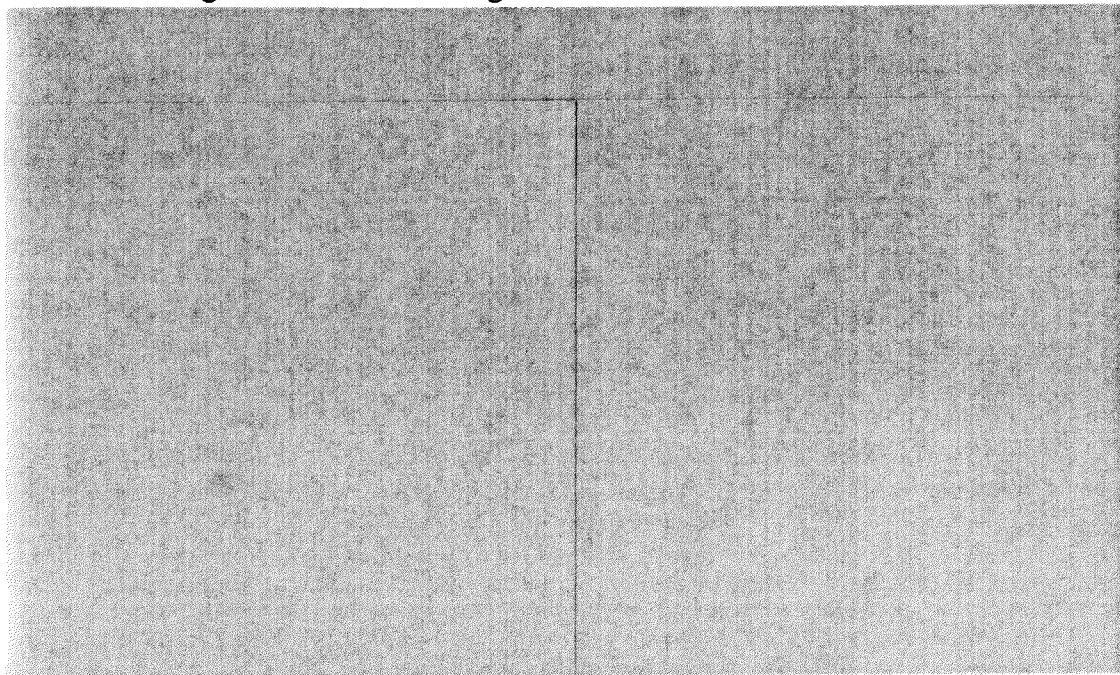
Address Changed to Reflect Correct Apartment Number



**Bank Routing Information**



**No Changes Made to bank Routing Information**





## OIG Penetration Testing Scorecard

Bureau	Vulnerabilities	Impact	Ease of Exploitation	Overall Penetrations Risk
BIA	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
BLM	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
BOR	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
OST	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
USGS	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
FWS	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
MMS	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
NBC	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
NPS**	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
OSM	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>

<input checked="" type="radio"/>	High
<input type="radio"/>	Medium
<input type="radio"/>	Low
<input type="radio"/>	Limited Testing

\*\*NPS  
Scorecard data for NPS is draft as risk rating has not been compiled as part of the report-based on analysts observations

This report is exempt from disclosure to the public under the Freedom of Information Act, under Exemption 2 of the Act, 5 U.S.C. § 552(b)(2). For this reason, recipients of this report must not show or release its contents for purposes other than official review and comment under any circumstances.

FOR OFFICIAL USE ONLY  
SECURITY SENSITIVE INFORMATION

# Penetration Testing Attachments

Master

### OIG Penetration Testing Scorecard

Bureau	Vulnerabilities	Impact	Ease of Exploitation	Overall Penetrations Risk
BIA				
BLM				
BOR				
OST				
USGS				
FWS				
MMMS				
NBC				
NPS**				
OSM				

	High
	Medium
	Low
	Limited Testing

Scorecard data for NPS is draft as risk rating has not been compiled as part of the report-based on analysts observations

This report is exempt from disclosure to the public under the Freedom of Information Act, under Exemption 2 of the Act, 5 U.S.C. § 552(b)(2). For this reason, recipients of this report must not show or release its contents for purposes other than official review and comment under any circumstances.

FOR OFFICIAL USE ONLY  
SECURITY SENSITIVE INFORMATION

## OIG Intrusion Detection Scorecard

Bureau	Internet Detection	Internal Detection	Traversal Detection
BIA	N/A	YES	N/A
BLM	YES	NO	NO
BOR	YES	NO	NO
OST	N/A	N/A	N/A
USGS	YES	NO	NO
FWS	YES	N/A	N/A
MMS	YES	N/A	N/A
NBC	NO	NO	NO
NPS	YES	NO	NO
OSM	NO	N/A	N/A
<b>Percentage</b>	<b>75%</b>	<b>17%</b>	<b>0%</b>

This report is exempt from disclosure to the public under the Freedom of Information Act, under Exemption 2 of the Act, 5 U.S.C. § 552(b)(2). For this reason, recipients of this report must not show or release its contents for purposes other than official review and comment under any circumstances.

FOR OFFICIAL USE ONLY  
SECURITY SENSITIVE INFORMATION