



OFFICE OF
INSPECTOR GENERAL
U.S. DEPARTMENT OF THE INTERIOR

SECURITY OF THE U.S. DEPARTMENT OF THE INTERIOR'S PUBLICLY ACCESSIBLE INFORMATION TECHNOLOGY SYSTEMS

This is a revised version of the report prepared for public release.




OFFICE OF
INSPECTOR GENERAL
U.S. DEPARTMENT OF THE INTERIOR

JUL 15 2015

Memorandum

To: Sylvia Burns
Chief Information Officer

From: Mary L. Kendall 
Deputy Inspector General

Subject: Final Evaluation Report – Security of the U.S. Department of the Interior’s
Publicly Accessible Information Technology Systems
Report No: ISD-IN-MOA-0004-2014

The Office of Inspector General has recently conducted an evaluation to assess cyber security defense measures for the U.S. Department of the Interior (Department). During our technical testing, we identified potential security weaknesses with the configuration of publicly available information technology systems at the Bureau of Reclamation, the Bureau of Safety and Environmental Enforcement, and the U.S. Geological Survey.

Our findings fall under two main categories; 1) inadequate understanding or testing of publicly available systems, and 2) missing controls that would protect internal systems in the event that those publicly available systems are compromised. The combination of these two findings can have wide-reaching impacts on the security of the Department’s information systems. The conditions can hide significant gaps within the Department’s security posture. This leads to questions about the processes used to make risk based decisions, such as those to authorize the operation of information systems. Current processes may be deficient due to insufficient risk awareness across the Department.

We offered six recommendations to assist the Department to address our findings. As the authority for information technology and security, it is the responsibility of the Office of the Chief Information Officer (OCIO) to guide and enforce security control mechanisms throughout the Department. In its response to our draft report, the OCIO concurred with all of our recommendations and stated that it is working to implement or close them (see Appendix 3). Based on this response, we consider the recommendations resolved, but not implemented (see Appendix 4), and we will forward them to the Office of Policy, Management and Budget to track their implementation.

The legislation creating the Office of Inspector General requires that we report to Congress semiannually on all audit, inspection, and evaluation reports issued; actions taken to implement our recommendations; and recommendations that have not been implemented.

If you have any questions about this report, please call me at 202-208-5745.

Table of Contents

Results in Brief	1
Introduction.....	2
Objective	2
Background	2
Technical Testing	3
Findings.....	5
Ineffective Measures for Identifying and Securing Publicly Accessible IT Systems.....	5
Missing Controls Puts Internal Systems and Sensitive Data at High Risk of Compromise	7
Conclusion and Recommendations.....	9
Conclusion.....	9
Recommendations Summary.....	9
Appendix 1: Scope and Methodology.....	12
Appendix 2: OWASP Categories.....	13
Appendix 3: Office of the Chief Information Officer’s Response to the Draft Report.....	15
Appendix 4: Status of Recommendations.....	18

Results in Brief

Defense in Depth is a widely recognized best practice for protecting critical information technology (IT) assets from loss or disruption by implementing overlapping security controls. The concept of Defense in Depth is that if one control fails then another is in place to either prevent or limit the adverse effect of an inevitable cyber attack. We found that three U.S. Department of the Interior (Department) Bureaus had not implemented effective Defense in Depth measures to protect key IT assets from Internet-based cyber attacks.

Specifically, we found nearly 3,000 critical and high-risk vulnerabilities in hundreds of publicly accessible computers operated by these three Bureaus. If exploited, these vulnerabilities would allow a remote attacker to take control of publicly accessible computers or render them unavailable. More troubling, we found that a remote attacker could then use a compromised computer to attack the Department's internal or non-public computer networks. The Department's internal networks host computer systems that support mission-critical operations and contain highly sensitive data. A successful cyber attack against these internal computer networks could severely degrade or even cripple the Department's operations, and could also result in the loss of sensitive data. These deficiencies occurred because the Department did not: 1) effectively monitor its publicly accessible systems to ensure they were free of vulnerabilities, or 2) isolate its publicly accessible systems from its internal computer networks to limit the potential adverse effects of a successful cyber attack.

Moreover, in recognition of increased cyber threats to Government systems, on May 21, 2015, the Department of Homeland Security (DHS) mandated that Federal agencies mitigate all critical vulnerabilities in publicly accessible systems within 30 days.¹ Using the DHS definition of critical vulnerability, we provided the results of our vulnerability testing, where we identified 668 critical confirmed vulnerabilities in various Bureaus' publicly accessible systems, to the affected Bureaus in January and February 2015, and OCIO in April 2015.

This report is the first in a series on Defense in Depth. We make six recommendations designed to mitigate identified vulnerabilities and strengthen security practices for the Department's network architecture and its public-facing edge, lessen the opportunity for a malicious attack, and minimize the impact and potential opportunities to infiltrate non-public systems after a successful attack.

¹ Department of Homeland Security Binding Operational Directive (BOD) 15-01 "Critical Vulnerability Mitigation Requirement for Federal Civilian Branch Departments and Agencies' Internet-Accessible Systems," May 21, 2015.

Introduction

Objective

We assessed the security of the U.S. Department of Interior's (Department) publicly accessible computers at three Bureaus. Specifically, we developed an inventory of publicly accessible computers operated by the three Bureaus and tested a sample for the presence of vulnerabilities which, if exploited, could allow a remote attacker to gain unauthorized access to Department systems and data. We also assessed the Bureaus' practices for managing and securing its inventory of publicly accessible computers.

Background

The Department spends about \$1 billion annually on its information technology (IT) asset portfolio—systems that support a range of Bureau programs that—

- protect and manage our Nation's natural resources and cultural heritage;
- provide scientific and other information to stakeholders interested in those resources; and
- help meet responsibilities to American Indians, Alaska Natives, and affiliated Island communities.

To support its diverse mission, the Department's IT asset portfolio contains hundreds of publicly accessible computers that enable Bureaus to share information with the public, collaborate with business and research partners and to provide their employees and contractors remote access to Department networks. Unfortunately, publicly accessible computers operated by Federal agencies are prime targets for exploitation and are highly sought after by criminals and foreign intelligence services.

The Department is a regular target of attacks both because of the large size of its networks and because those networks contain technical and other sensitive information highly sought after by criminals and foreign intelligence services. In addition, the Department's substantial connectivity with outside organizations makes it essential that the Department protect its network to prevent sophisticated attackers from using a security flaw in a system to gain unauthorized access to other interconnected computer networks.

Over the past few years, hackers and foreign intelligence services have compromised the Department's computer networks by exploiting vulnerabilities in publicly accessible systems on at least 23 occasions. Exact figures were not available because of incomplete supporting documentation regarding the exact disposition of recorded incidents. These security incidents resulted in the loss of sensitive data and disruption of Bureau operations. Notable examples include:

- In October 2014 and December 2014, hackers exploited vulnerable publicly accessible systems to steal user credentials with privileged (administrative) access to Department systems. Although the extent of these system breaches was never fully determined, with administrative access to a computer system, an attacker can: 1) copy, modify, or delete sensitive files; 2) add, modify, or delete user accounts; 3) upload hacking tools or malware to steal user credentials and compromise other departmental systems; and 4) modify system logs to conceal their actions to maintain a presence inside the Department's networks for future exploits. In other words, in these two attacks, the intruders could have gained full functional control over Department systems.
- An October 2014 attack originating from European-based Internet-protocol (IP) addresses resulted in the loss of an unknown amount of data when the attackers gained control of two of the Department's public web servers.²
- A May 2013 attack originating from Chinese-based Internet-Protocol (IP) addresses where the attackers kept a sustained presence inside the Department's network. In the 4 weeks before the Department fully contained the security breach, the attackers had stolen an unknown amount of data and had uploaded malware which would have allowed for the compromise of other systems.

Measures to effectively manage and secure an organization's public IT systems include: 1) initializing systems to a secure state before deployment; 2) identifying and maintaining accurate system inventories; 3) regular vulnerability testing and timely mitigation of all critical and high-risk vulnerabilities; 4) periodic reviews to consolidate or eliminate duplicative and unused systems; and 5) isolating publicly accessible systems from internal computer networks to prevent a remote attacker from using a vulnerability in an organization's public-facing systems to compromise the entire organization.

Technical Testing

As part of a broader evaluation to gauge the effectiveness and capabilities of Defense in Depth security strategies for IT systems within the Department, we conducted technical testing of publicly available websites for three Bureaus.

The Department's total number of publicly accessible computers is unknown because the Department does not regularly perform discovery scans of its public IP address space to develop and maintain an inventory of them.

² An Internet Protocol address or IP address is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication. Internet Protocol is a communications protocol or set of standard rules used to transmit data over the Internet. The most widely used protocol on the Internet today is IP Version 4, which provides about 4.3 billion IP addresses for use worldwide.

During the testing, we were able to compromise two websites. During this compromise, we gained access to two different servers. With no additional malicious efforts, we enumerated services that are not made available to the public. Due to the nature of the compromise, we notified the Bureau within minutes of the breach. The immediate notification severely limited further testing regarding the opportunities to navigate between Bureaus.

While we only gained access through two servers, we found that other websites were vulnerable to more advanced attack techniques. We did not exploit these attack vectors in order to minimize impact to the Bureaus. The discovered weaknesses were delivered via technical reports and out briefings to the respective Bureaus. In regard to the Department's website security program, we found an absence of secure configuration guidance and enforcement, no inventory for publicly available services, and an ineffectual security testing process. We also found that the impact of these problems is magnified by insecure network architecture and the absence of internal traffic monitoring and analysis.

Findings

Our findings fall under two main categories—inadequate understanding or testing of publicly available systems and missing controls that would protect internal systems in the event that those publicly available systems are compromised. The combination of these two findings can have wide-reaching impacts on the security of the Department’s information systems. The conditions can hide significant gaps within the Department’s security posture. This leads to questions about the processes used to make risk based decisions, such as those to authorize the operation of information systems. Current processes may be deficient due to insufficient risk awareness across the Department.

Ineffective Measures for Identifying and Securing Publicly Accessible IT Systems

The Department’s publicly accessible systems are prime targets for exploitation, and thus are highly sought after by hackers. To determine the extent to which publicly accessible computers operated by three Bureaus were vulnerable to an Internet-based attack, we conducted a test to probe their computer networks.

At the time of our test, we found that 78% of the publicly accessible IP addresses were used to host publicly accessible websites. In some instances, the same IP address (e.g., computer) offered multiple publicly accessible services.

Because websites comprised the majority of the three Bureaus’ publicly accessible computers, we tested for the presence of vulnerabilities, which a remote attacker could exploit to gain unauthorized access to Department computer systems and data.

The types of vulnerabilities discovered included command and structured query language injection, cross-site scripting, security misconfiguration, sensitive data exposure and others. Because exploiting these vulnerabilities often results in data loss or adverse effects on the availability and integrity of affected systems, Open Web Application Security Project (OWASP) categorizes them as either critical or high-risk and recommends organizations make mitigation a priority.

We provided the results of our vulnerability testing as separate reports addressed to the responsible IT personnel at the affected Bureaus for action. The high number of vulnerabilities detected occurred because the same security flaw often affected many websites

As a result of interviews with the Office of the Chief Information Officer (OCIO) and Bureau IT personnel and our technical testing, we found that the Department is unaware of the number of its publicly accessible IT systems or whether those systems are free from vulnerabilities. Although the Department maintains an overall inventory of its portfolio of IT systems, it cannot identify which systems

are accessible over the Internet. Moreover, the Department was also unable to tell us which of its publicly accessible systems contained sensitive data or supported critical Bureau operations. Knowing which publicly accessible computers, if exploited, would expose confidential data or adversely affect Bureau operations would help the Department prioritize resources to ensure that its most critical publicly accessible IT assets are adequately secured.

The Department performs vulnerability scanning service for externally available IP addresses. An off-the-shelf scanning tool is configured to use default vulnerability checks without performing any advanced or context based testing such as web application testing, credentialed testing, replay attacks, data content review, exploits, etc. Automated scans with default settings are ineffective for detecting most security flaws in web applications, which is frequently due to insecure custom coding practices, authentication mechanisms, custom input requirements, and divergent delivery sources. Advanced testing methodologies allow for a much greater depth of weakness discovery.

Data from vulnerability scanning is available to the Bureaus but results are not routinely used by the Department to review or enhance perimeter security controls, such as ensuring discovered vulnerabilities are mitigated in a timely manner.

The scanning and reporting process is automated. The Bureaus are expected to independently access, assess, and mitigate any results. The Department does not enforce Bureau participation. Without advanced testing, trend analysis, and review of the results, this vulnerability scanning service does not effectively monitor publicly accessible systems to ensure they remain free of vulnerabilities.

We also found that the Department does not test new services prior to making them available to the public. Instead, the Department expects system owners to do this task without a prescribed methodology. Initializing a Federal agency's publicly accessible systems, such as its public websites, to a secure state before deployment helps ensure these systems are not exploited. Moreover, regular monitoring of an agency's publicly accessible computers for technical vulnerabilities and timely patching are widely recognized best practices that increase the effectiveness of an organization's IT security program by finding and fixing vulnerabilities before they are exploited. Having accurate, up-to-date inventories of publicly accessible systems is a control that helps the agency ensure that all of its public-facing systems are regularly monitored.

Because of these control deficiencies, there is a high risk that vulnerabilities allowing a remote attacker to gain unauthorized access to the Department's publicly accessible systems and data would go undetected and uncorrected.

Recommendations

We recommend that the Department's Chief Information Officer:

1. Require and enforce the secure development and management of all publicly available IT services, to include:
 - a. an official approval process;
 - b. cloud candidacy evaluation;
 - c. testing requirements;
 - d. architectural designs and data flow;
 - e. minimum layered security controls; and
 - f. standardized platforms and utilities.
2. Perform periodic discovery activities and reconcile results with approved inventory of Bureau and Department services to include:
 - a. all service site URLs;
 - b. all public IP ranges; and
 - c. identification of public systems housing sensitive or mission-critical data.
3. Expand existing external vulnerability scanning services to include the following:
 - a. advanced service exploit testing;
 - b. advance website (URL-based) exploit testing;
 - c. oversight of remediation activities to include:
 - i. develop and enforce guidelines for mitigation timeliness that comply with DHS Binding Operational Directive 15-01;
 - ii. tracking and validation of implemented solutions;
 - iii. all external weakness identified by Bureaus, OCIO, Office of Inspector General (OIG), or other third parties; and
 - d. trend analysis.

Missing Controls Puts Internal Systems and Sensitive Data at High Risk of Compromise

We found that the Department did not isolate publicly accessible systems from internal computer networks. Compromising a Department public web server by itself may not result in disrupting mission-critical operations or in the loss of sensitive information. The National Institute of Standards and Technology (NIST) recommends that organizations implement controls to isolate (prevent communication between) their publicly accessible computers from computers on the organization's internal network. Thus, even if attackers take control of a public web server, network isolation will prevent them from accessing the internal

network. NIST also recommends alerting the organization's incident response team of all attempted connections from the web server to the organization's internal network. Such traffic is most likely malicious and may indicate that the web server has been compromised. Implementing these recommended security measures demonstrates the Defense in Depth concept in information security—protecting an organization's critical IT assets with a series of security controls such that if one control fails—another is in place to either prevent or limit the adverse effect of an attack.

In addition, due to the absence internal traffic monitoring and filtering, this failure to adequately isolate publicly available systems expands the impact of any single attack beyond each Bureau to the Department network as a whole.

Recommendations

We recommend that the Department's Chief Information Officer:

4. Require all publicly available systems to be hosted in an isolated infrastructure.
5. Perform periodic advanced testing to validate the effectiveness of controls in isolating public systems from internal systems.
6. Implement an intrusion monitoring solution that can analyze and correlate internal traffic patterns and detect attack signatures across Bureaus, including the capability for active traffic interception.

Conclusion and Recommendations

Conclusion

The cyber security of the Department suffers in main part due to inadequate centralization of policy, guidance, and enforcement. While the Department's Chief Information Officer regularly distributes memoranda requiring security measures be put in place, it does not mandate details on how those security measures should be deployed, tested, or enforced on a regular basis. Inadequate guidance has resulted in a wide array of solutions that cannot easily be monitored and tested for efficiency. In addition, an unbalanced culture of business over security has resulted in the widespread removal of internal security segmentation and monitoring programs. Mission is priority, but as seen with the recent U.S. Office of Personnel Management incident involving the Department's shared hosting service, it must not be achieved at the expense of security.

Due to disparate solutions among the Department and Bureaus, the OCIO is unaware of the breadth of publicly available systems and the communication methods with the Internet or the ESN. The OCIO is unable to adequately measure or enforce security solutions protecting its data. Without a greater understanding of the systems or the methods employed to protect them, authorizing officials cannot adequately understand the level of risk of operating in this environment.

Our findings reflect an absence of a centralized capability for defining and measuring security controls that protect the Department. The absence of several common internal security mechanisms exacerbate our findings to an unacceptable level, which poses a great risk to departmental systems. All departmental systems connected via the ESN may be operating under a false level of confidence in the security controls shared with the Department and Bureaus. Our recommendations are aimed at helping the OCIO increase its involvement in the security measures employed throughout the Department and re-evaluate its network architecture for inadequate isolation techniques and an absence of internal monitoring and segmentation.

Recommendations Summary

We recommend that the Department's Chief Information Officer:

1. Require and enforce the secure development and management of all publicly available IT services, to include:
 - a. an official approval process;
 - b. cloud candidacy evaluation;
 - c. testing requirements;
 - d. architectural designs and data flow;
 - e. minimum layered security controls; and
 - f. standardized platforms and utilities.

OCIO Response

In its response to our draft report, OCIO concurred with this recommendation.

2. Perform periodic discovery activities and reconcile results with approved inventory of Bureau and Department services to include:
 - a. all service site URLs;
 - b. all public IP ranges; and
 - c. identification of public systems housing sensitive or mission-critical data.

OCIO Response

In its response to our draft report, OCIO concurred with this recommendation.

3. Expand existing external vulnerability scanning services to include the following:
 - a. advanced service exploit testing;
 - b. advance website (URL-based) exploit testing;
 - c. oversight of remediation activities to include:
 - i. develop and enforce guidelines for mitigation timeliness that comply with DHS Binding Operational Directive 15-01;
 - ii. tracking and validation of implemented solutions;
 - iii. all external weakness identified by Bureaus, OCIO, OIG, or other third parties; and
 - d. trend analysis.

OCIO Response

In its response to our draft report, OCIO concurred with this recommendation

4. Require all publicly available systems to be hosted in an isolated infrastructure.
- 5.

OCIO Response

In its response to our draft report, OCIO concurred with this recommendation.

5. Perform periodic advanced testing to validate the effectiveness of controls in isolating public systems from internal systems.

OCIO Response

In its response to our draft report, OCIO concurred with this recommendation.

6. Implement an intrusion monitoring solution that can analyze and correlate internal traffic patterns and detect attack signatures across Bureaus, including the capability for active traffic interception.

OCIO Response

In its response to our draft report, OCIO concurred with this recommendation

We consider these six recommendations resolved but not implemented, and we will refer them to the Office of Policy, Management and Budget to track their implementation. See Appendix 3 for the full text of the OCIO's response. Appendix 4 lists the current status of our recommendations.

Appendix I: Scope and Methodology

Scope

For this evaluation, our work was limited to the specific procedures and analysis described in the Rules of Engagement completed with each Bureau, and was based only on the information made available through November 21, 2014.

Methodology

To accomplish our evaluation objectives, we performed the following procedures:

- Interviews with subject matter experts at the Office of the Chief Information Officer and the three Bureaus;
- Automated public resource discovery scanning;
- Automated public resource vulnerability scanning;
- Manual website vulnerability testing; and
- Analysis of findings.

We conducted this evaluation in accordance with the Quality Standards for Inspection and Evaluation as put forth by the Council of Inspectors General on Integrity and Efficiency. We believe that the work we performed provides a reasonable basis for our conclusions and recommendations.

Appendix 2: OWASP Categories

The Open Web Application Security Project (OWASP) maintains a popular annual industry standard definition of the top 10 security flaws affecting websites today. OWASP is focused on the improvement of software security, and maintains a list of the 10 most critical web application security flaws. The weaknesses we found were distributed across 6 of OWASP's Top 10 flaws for 2013. OWASP defines these five weaknesses (see Figure 1) as³:

- **A1-Injection:** “Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker’s hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.”
- **A3-Cross-Site Scripting (XSS):** “XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim’s browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.”
- **A5-Security Misconfiguration:** “Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date.”
- **A6-Sensitive Data Exposure:** “Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.”
- **A8-Cross-Site Request Forgery (CSRF):** “A CSRF attack forces a logged-on victim’s browser to send a forged HTTP request, including the victim’s session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim’s browser to generate requests the vulnerable application thinks are legitimate requests from the victim.”
- **A9-Using Components with Known Vulnerabilities:** “Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications

³ https://www.owasp.org/index.php/Top_10_2013-Top_10.

using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.”

Appendix 3: Office of the Chief Information Officer's Response to the Draft Report

The OCIO's response to our draft report follows on page 16.




United States Department of the Interior

OFFICE OF THE SECRETARY

Washington, DC 20240

JUL 9 2015

To: Kimberly Elmore
Assistant Inspector General for Audits, Inspections, and Evaluations

From: Sylvia Burns
Chief Information Officer 

Subject: Office of Inspector General, Draft Evaluation Report, Security of the
U.S. Department of the Interior's Publicly Accessible Information Technology
Systems, Report No. ISD-IN-MOA-0004-2014

The Department of the Interior (Department), Office of the Chief Information Officer (OCIO), appreciates the opportunity to review the Office of Inspector General (OIG) draft Evaluation Report (Report), Security of the U.S. Department of the Interior's Publicly Accessible Information Technology (IT) Systems, ISD-IN-MOA-0004-2014. Attachment 1 provides the Department's Corrections and Comments to the draft Report. Attachments 2 and 3 provide the Department's Summary Response and the OCIO Statement of Actions to implement the OIG's draft recommendations. They serve as a preview of our formal response given the contents of the draft Report. The Department will update these attachments as appropriate based on the OIG's final Report.

The Department supports and appreciates the OIG's work in assessing and advising on the potential vulnerability of its information technology systems to outside intrusions. This vulnerability assessment provides valuable information about potential vulnerabilities that assists greatly in the Department's ongoing efforts to strengthen data security. Accordingly, the Department and its bureaus fully cooperated with the OIG upon being advised of this assessment. The Department accepts the OIG's recommendations, and will incorporate them into a Departmental cyber security action plan. Further, the Department is engaging all bureaus and offices in discussions about the OIG's findings and the need to undertake major changes in how we manage publicly facing systems across the entire Department. The impacted bureaus report that the vulnerabilities identified in the Report have been corrected or are in the process of being addressed. The OCIO will monitor the correction of any remaining vulnerabilities and require the impacted bureaus to resolve them within the next 30 days.

OCIO recently established a Department-wide cyber security advisory group with experts from a variety of IT management disciplines. The group will advise and support the CIO in developing and implementing a comprehensive, multi-pronged, cyber security strategy and action plan for the agency. The plan will include short, medium and long-term initiatives to strengthen the Department's IT security posture. In addition, the Department's ongoing implementation of Secretarial Order 3309, Information Technology Management Functions and Establishment of Funding Authorities, and the Federal Information Technology Acquisition Reform Act

(FITARA), will address many of the longstanding challenges in IT management identified by the OIG.

The Department appreciates the OIG's evaluation of the security of the Department's publicly accessible computers and its objective perspective on our IT security posture in the interest of promoting excellence, integrity, and accountability in our IT program, operations, and management.

If you have any questions, please contact me at (202) 208-6194 or sylvia_burns@ios.doi.gov. Staff may contact Steven B. Thompson, Acting Director, Internal Control, Audit, and Compliance Management at (202) 821-8887, or steven_thompson@ios.doi.gov.

Attachments:

1. Corrections and Comments to the Office of Inspector General's Draft Evaluation Report
2. Department's Summary Response
3. OCIO Statement of Actions to Address Office of Inspector General Draft Evaluation Report U.S. Department of the Interior's Adoption of Cloud Computing Technologies Report No. ISD-IN-M-OA-0004-2014

Appendix 4: Status of Recommendations

In its response to our draft report, the Office of the Chief Information Officer concurred with our six recommendations and stated that it was working to implement or close them. The response included target dates and an action official for each recommendation (see Appendix 3). We consider these recommendations resolved but not implemented.

Recommendations	Status	Action Required
1, 2, 3, 4, 5, 6	Resolved but not implemented	We will refer these recommendations to the Office of Policy, Management and Budget to track their implementation.

Report Fraud, Waste, and Mismanagement



Fraud, waste, and mismanagement in Government concern everyone: Office of Inspector General staff, departmental employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and mismanagement related to departmental or Insular Area programs and operations. You can report allegations to us in several ways.



By Internet: www.doi.gov/oig/index.cfm

By Phone: 24-Hour Toll Free: 800-424-5081
 Washington Metro Area: 202-208-5300

By Fax: 703-487-5402

By Mail: U.S. Department of the Interior
 Office of Inspector General
 Mail Stop 4428 MIB
 1849 C Street, NW.
 Washington, DC 20240