



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

U.S. DEPARTMENT OF THE INTERIOR WEB HOSTING SERVICES

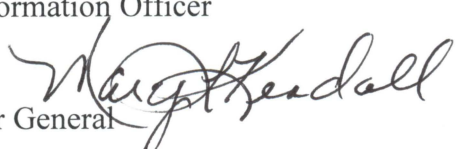


OFFICE OF
INSPECTOR GENERAL
U.S. DEPARTMENT OF THE INTERIOR

JUN 04 2014

Memorandum

To: Sylvia Burns
Acting Chief Information Officer

From: Mary L. Kendall 
Deputy Inspector General

Subject: Inspection Report – U.S. Department of the Interior Web Hosting Services
Report No. ISD-IS-OCIO-0001-2014

In early January 2014, the U.S. Department of the Interior (DOI) and Office of Inspector General (OIG) websites experienced an extended outage of 7 days. These websites, which are hosted by the National Park Service (NPS), provide critical information to the general public, and their availability contributes to the missions of both DOI and OIG. We initiated an inspection to determine the cause of the outage and to identify whether the length of the recovery was appropriate.

During our inspection, we uncovered multiple reasons and deficiencies that contributed to the website outage at NPS, DOI, and OIG. These included NPS information systems that—

- had not been properly authorized to operate;
- had outdated system inventories and were missing security documentation; and
- had insufficient contingency planning to prepare for a major power failure.

In addition, we found that no written agreements existed between NPS, DOI, and OIG describing the roles and responsibilities of each entity.

Background

NPS has over 400 locations throughout the United States whose interconnected networks and computer systems are known as the NPS One General Support System (One GSS). NPS has a web hosting and content management system in its Lakewood, CO, data center referred to as the Denver Data Center Child System (DDC) that manages the content for NPS' and DOI's websites.¹ According to the DDC's system documentation, the DDC is a subsystem (child) of One GSS. NPS contracts with a Cloud-based content delivery network (CDN)² provider that delivers NPS and DOI web content to the public. Under a 2009 verbal agreement, NPS agreed to

¹The DDC hosts several other DOI websites, including, but not limited to, OIG, the Office of the Secretary, and the Office of the Solicitor. Most DOI bureaus, however, do not use NPS or DOI for web hosting services and were not affected by this outage.

²A CDN is an interconnected system of computers on the Internet that provides website content rapidly to numerous users by duplicating the content on multiple geographically distributed servers and directing the content to users based on proximity.

host the DOI website in the DDC and continuously maintain the content hosted by the CDN. After an extended outage of the OIG website in 2012, DOI's Office of Communications suggested that OIG allow DOI to host and manage the OIG website. OIG verbally accepted DOI's offer in 2012 to share web hosting and content management services, thus migrating OIG's website to DDC; NPS, however, was not informed of this decision.

On January 1, 2014, the DDC experienced a power outage that affected over 100 servers and, in some cases, caused physical damage. As a result of the outage, the DOI and OIG websites were unavailable between January 1 and January 7, 2014.

In response to the outage, on January 3, 2014, DOI uploaded a temporary web page to the CDN that contained links to the bureau websites unaffected by the outage. Although NPS hosts the OIG website, it does not host the OIG hotline web page; therefore, the hotline page was unaffected by the outage. DOI did not include a link to the hotline page on the temporary web page.

Findings

Our inspection revealed several concerns with DOI's web hosting services, including insufficient assessment and authorization processes and incomplete documentation, noncompliance with contingency planning and testing requirements, and no written documentation identifying the roles and responsibilities for shared services.

Insufficient Assessment and Authorization Processes and Incomplete Documentation

During our inspection, we could not determine whether the information systems hosting the NPS, DOI, and OIG websites were included in the One GSS assessment and authorization (A&A) boundary, as required by the Federal Information Security Management Act of 2002, because NPS did not have accurate system inventory documentation. In addition to incomplete system inventories for identified information system boundaries, we discovered insufficient contingency planning processes, an unauthorized information system, missing baseline configuration documentation, and a variety of other missing documentation.

An A&A boundary establishes the scope of protection for organizational information systems and includes the people, processes, and information technologies that are part of the system. Incomplete documentation of the One GSS boundary represents NPS' inadequate assessment of the system and the data the system hosts. As a result of insufficiently following A&A processes defined by Federal regulations and noncompliance with security documentation requirements (see Appendix 1), we cannot rely on the annual assurance statement that NPS signed supporting continuing authorization to operate for One GSS and the DDC.

According to the National Institute of Standards and Technology (NIST) every component of an information system must be a member of an identified information system boundary to obtain authorization to operate and that up-to-date system inventories, including identification of parent and child system relationships, are essential to providing authorizing officials an accurate and complete understanding of the system (see Appendix 1). We found that

the servers hosting the DOI and OIG websites appeared to be included in the system inventory of the DDC A&A boundary, but NPS did not clearly document the parent-child relationship between One GSS and the DDC. Although the DDC identified itself as a child of the One GSS information system boundary, One GSS did not identify the DDC as a child system. Therefore, One GSS did not include the DDC and its components in its system inventory. In addition, documentation for One GSS, including system and inventory documentation, was not kept up to date. As a result, NPS did not know that the DDC hosted the OIG website and therefore did not include it in the One GSS system inventory.

We also found that One GSS only inventories systems monitored with Microsoft System Center Configuration Manager (SCCM). SCCM, however, generates an incomplete system inventory for One GSS because it excludes all non-Microsoft components. NPS configured SCCM to inventory and manage only Microsoft computers and servers, but other documentation for the One GSS boundary indicated the existence of several non-Microsoft components, including network equipment, websites, and data types. According to NIST, a system inventory should include the entire environment of the operation, including all components of the information system. NPS only used data from SCCM as documentation for the One GSS inventory, making the One GSS inventory wholly incomplete.

In addition, we determined that the CDN had not been authorized to operate because NPS incorrectly believed that contractor systems were not required to be included within an information system boundary and undergo A&A. NIST and DOI criteria require that all systems, including contractor systems, operate through the A&A process (see Appendix 1). We also found that the CDN's baseline configuration for the DOI and OIG websites was set to refresh content every 6 hours, which is a short-lived setting in comparison to the 30-day refresh setting for the NPS website. Due to the power outage, the CDN could not communicate with the DDC during its refresh interval; the CDN interpreted the outage as an intentional update and purged the DOI website, which subsequently purged the OIG website. NPS reported that it had no baseline configuration documentation to identify why the 6-hour refresh for the DOI and OIG websites was set within the CDN.

Baseline configurations determine the security control selection process, but NPS could not provide us with baseline information for the CDN. Baselines provide a starting point for evaluating the overall risk of the information system and are established after the system owner and the owner's staff have formally reviewed and agreed upon them. Established baseline configurations and appropriate change control procedures facilitate the risk management process to identify and accept or mitigate the risks associated with deviating from that baseline. An appropriate A&A package for the CDN should have included a detailed description of system connections and data flow processes and may have alerted NPS to the risk associated with the short-lived baseline configuration for refreshing the content of the DOI and OIG websites.

Lastly, we could not determine which system security plan was authoritative for the DDC because NPS manually created, externally maintained, and uploaded its system security plan to the Cyber Security Assessment and Management (CSAM) tool instead of using the automated report generation capability. CSAM is a system used for managing A&A packages that has the capability to automatically create and make updates to the system security plan by incorporating

all of the latest system updates as input by the system owner. DOI regulations require all systems to use CSAM as the authoritative repository for all A&A documentation (see Appendix 1).

We identified several other required documents missing from CSAM, including—

- contingency plan test results;
- a continuous monitoring plan;
- a business impact assessment;
- a risk assessment report; and
- results from quarterly control assessments.

As a result of insufficient A&A processes and incomplete security documentation, NPS could not have effectively set priorities and managed risk according to the NPS, DOI, or OIG risk strategies. NPS officials could not have made a fully informed decision to grant authorization to operate to One GSS using the available information.

Noncompliance With Contingency Planning and Testing Requirements

NPS could have been better prepared to efficiently respond to and minimize damage and downtime from the outage if it had an appropriate contingency plan in place. NIST guidance requires bureaus and offices to test contingency plans annually (see Appendix 1). These plans help ensure adequate preparation to cope with the loss of operational capabilities due to a service disruption, such as an act of nature, fire, accident, or sabotage. According to NIST, these plans should cover all key functions, including assessing an agency's information technology and identifying resources, minimizing potential damage and interruption, developing and documenting the plan, and testing the plan and making necessary adjustments.

Our inspection found that the One GSS contingency plan had not been reviewed or updated since December 11, 2008. CSAM did not have contingency plan test documentation for the One GSS boundary, which indicates that the plan has never been tested. Contingency planning is another component of the risk management framework that establishes thorough plans, procedures, and technical measures that enable quick and effective system recovery following a service disruption.

NPS documentation stated that the DDC contingency plan has been tested annually as required, but we concluded that the tests conducted were inadequate. For example, the DDC test conducted on June 13, 2013, tested NPS' security incident response capability to an unauthorized user but not its capability to recover from an outage. Moreover, the DDC test conducted on January 10, 2012, tested the validity of the backups for restoring a single server, but the severity of the scenario did not trigger activation of the plan. Since neither test scenario activated the contingency plan, NPS had not conducted appropriate testing and was therefore unprepared to respond to the consequences of the outage.

We also determined that the DDC did not have adequate backup power for the number of servers, workstations, and routers it supports to minimize physical damage to equipment. The battery backup only lasted approximately 30 minutes, which was not enough time for NPS

personnel to power down the servers. NPS stated that it did not have a shutdown plan or an automated shutdown capability, which resulted in damage to multiple servers. Basic physical and environmental protections are required by NIST for the protection of equipment in information system boundaries such as One GSS and DDC (see Appendix 1).

No Written Documentation Identifying the Roles and Responsibilities for Shared Services

Lastly, we determined that NPS, DOI, and OIG do not have written agreements for website hosting, system ownership, support to contingency planning, recovery timeframes, or funding. NPS hosts the DOI website under a verbal agreement made in 2009 between individuals that no longer work for DOI, and DOI's Office of Communications does not know the terms of that agreement. In addition, in 2012, OIG verbally agreed to transfer the hosting and content management services of its website to DOI. Prior to this inspection, OIG did not know that NPS hosted either the DOI or OIG website.

Our inspection revealed that NPS and DOI disagree over ownership of the system boundary that covers DOI's website, ownership of the data, and the importance of the websites' availability to the public. The prevailing attitude of NPS officials appeared to indicate that a timely recovery of the DOI website was not their priority. Appropriate documentation, such as a memorandum of understanding or a service level agreement, that defined the roles and expectations for NPS, DOI, and OIG, would have alleviated disagreement among the three parties, and each entity would have had a clear understanding of its responsibilities related to web hosting and content management services, including the prioritization of system restoration in the event of a major outage.

Recommendations

We recommend that DOI's OCIO and Office of Communications:

1. Establish an oversight process to review and improve the effectiveness of A&A activities within DOI;
2. Establish a review process for determining the validity of annual assurance statements;
3. Establish an oversight process to enforce proper CSAM use for all systems;
4. Assess the risk of continuing to host DOI data at the DDC based on NPS' A&A activities; and
5. Document and approve appropriate service level requirements and operational and security role expectations for continued use of NPS' hosting services.

We recommend that NPS:

1. Perform an accurate A&A for the CDN, the DDC, and One GSS following all applicable laws, regulations, and requirements to continue to operate;
2. Establish a process to identify systems with inadequate A&A;
3. Upload all system documentation for all information systems, including the CDN, the DDC, and One GSS, to CSAM immediately after approval;
4. Establish a process to enforce proper CSAM use for all NPS systems;
5. Perform a new business impact analysis for both the DDC and One GSS based on customer data and recovery time objectives;
6. Update contingency plans incorporating customer recovery time objectives and expectations, accurate system inventories, and lessons learned from the recent outage;
7. Update the facility power capabilities or migrate the web hosting platform to a facility that meets physical and environmental requirements if NPS is required to meet customer recovery time objectives and expectations;
8. Design and conduct annual contingency plan tests; and
9. Document in writing and approve all agreements for providing web hosting services.

Please provide us with your written response to this report within 30 days. The response should provide information on actions taken or planned to address the recommendations, as well as target dates and title(s) of the official(s) responsible for implementation. Please send your response to:

Kimberly Elmore
Assistant Inspector General
Office of Audits, Inspections, and Evaluations
U.S. Department of the Interior
Office of Inspector General
Mail Stop 4428
1849 C Street, NW.
Washington, DC 20240

Scope and Methodology

We focused our inspection on DOI, OIG, and NPS website hosting associated with the website outages in early January 2014. We reviewed the NPS services at the NPS data center in Lakewood, CO, and interviewed staff at DOI's Office of the Chief Information Officer, DOI's Office of Communications, NPS, and OIG. We also observed the physical environment at the NPS data center. Lastly, we reviewed Federal requirements for information systems and relevant

DOI, NPS, and OIG security documentation, policies, and procedures related to information security. We conducted this inspection in January 2014.

Although we included OIG data as part of the inspection sample, we conducted our inspection in accordance with the Quality Standards for Inspection and Evaluation as put forth by the Council of the Inspectors General on Integrity and Efficiency. We believe that the work performed provides a reasonable basis for our conclusions and recommendations.

OIG was not exposed to any undue influence during this assignment. Following our standard inspection procedures, OIG management was not involved in the daily activities of the inspection but did review and approve the working papers. The inspection team executed our internal procedures of indexing and referencing their findings, which involves linking the statements in the report to specific working papers and having an independent referencer verify the indexes to support all facts, figures, and findings. These review controls ensured that OIG remained independent and that the inspection was conducted in accordance with the Quality Standards.

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 regarding this report, please contact me at 202-208-5745.

cc: NPS Information Officer
DOI Office of Communications

Federal and Agency Policies and Procedures

Federal Law, Policy, Standards, and Guidance

- **Federal Information Security Management Act of 2002 (FISMA):** FISMA establishes the information security responsibilities of the head of each agency. This includes the responsibility for the security of any information system used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. Under FISMA, the National Institute of Standards and Technology (NIST) is tasked with developing standards and guidelines. FISMA requires regular review and testing of all policies, procedures, and practices.
- **Office of Management and Budget (OMB) Memo 11-33, “Fiscal Year 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management,” September 14, 2011:** OMB Memo 11-33 discusses the change from annual certification and accreditation to an ongoing risk-based approach to assessment and authorization (A&A) for ensuring the security of Federal information systems.
- **OMB Memo 14-03, “Enhancing the Security of Federal Information and Information Systems,” November 18, 2013:** OMB Memo 14-03 establishes timelines for the requirement to migrate to the risk management framework and continuous monitoring model used for ongoing A&A.
- **Federal Information Processing Standards (FIPS) Publication 199, “Standards for Security Categorization of Federal Information and Information Systems,” February 2004:** Agencies first categorize their information and systems as required by FIPS 199. This helps to ensure that appropriate security requirements and security controls are applied to all Federal information and information systems including Cloud computing.
- **FIPS Publication 200, “Minimum Security Requirements for Federal Information and Information Systems,” March 2006:** After completing the categorization process in FIPS 199, agencies are then required to select an appropriate set of security controls from NIST Special Publication 800-53 to satisfy minimum security requirements. FIPS 200 and NIST Special Publication 800-53 help ensure that appropriate security requirements and security controls are applied to all Federal information and information systems. The assessment of risk determines the initial security control selection and determines if any additional controls are needed to protect organizational operations (including mission, functions, image, or reputation). The resulting set of required security controls establishes a level of security due diligence for the organization.
- **NIST Special Publication 800-53 Revision 3, “Recommended Security Controls for Federal Information Systems and Organizations,” August 2009, includes updates as of May 1, 2010:** NIST Special Publication 800-53 defines all security controls applicable to Federal information systems and covers the steps in the risk management framework

that address security control selection. In this document, security controls related to 18 security control families are available for organizations to select when they undergo the FIPS 200 control selection process. Each security control family contains the specific security controls related to the security functionality of the family, including security assessment and authorization, contingency planning, physical and environmental protection, and risk assessment.

- **NIST Special Publication 800-37, “Guide for Applying the Risk Management Framework to Federal Information Systems,” February 2010:** The risk management framework (RMF) describes a disciplined and structured process that integrates information security and risk management activities into the system development life cycle. The RMF defines an authorization boundary and states that all components of an information system be authorized for operation by an authorizing official. Initial authorization to operate is based on evidence available at one point in time, but systems and environments of operation change. Ongoing assessment of security control effectiveness supports a system’s security A&A over time in highly dynamic environments of operation with changing threats, vulnerabilities, technologies, and missions and business processes. The RMF is the process for obtaining system authorization and, more generally, for managing and continually monitoring information security and information system-related risk.
- **NIST Special Publication 800-137, “Information Security Continuous Monitoring for Federal Information Systems and Organizations,” September 2011:** NIST Special Publication 800-137 states that agencies must develop information security continuous monitoring (ISCM) activities that include multiple tiers of an organization. There are different responsibilities for each tier in order for a system to obtain authorization to operate and each tier must continually monitor security controls to maintain that authorization. The ISCM process must also include organizationally determined assessment and monitoring frequencies. Through ISCM, new threat or vulnerability information is evaluated as it becomes available, permitting organizations to make adjustments to security requirements or individual controls as needed to maintain authorization decisions.

DOI Policy and Guidance

- **Office of the Chief Information Officer (OCIO) Directive 2011-006, “Information System Boundary Assessment & Authorization Package Documentation and Inventory,” March 23, 2011:** OCIO Directive 2011-006 establishes Cyber Security Assessment and Management (CSAM) as the official repository for all A&A documentation and provides instructions to bureaus for the proper use of the system. It also provides detailed guidance on how to establish information system and subsystem boundary relationships between general support systems, major applications, and minor applications.
- **OCIO Memorandum 0000228, “Ongoing Assessment and Authorization Through Continuous Monitoring,” March 16, 2012:** CIO 0000228 redefines the certification and

accreditation guidance to be called the A&A process and requires the implementation of the risk management framework and continuous monitoring instead of conducting annual reauthorizations.

- **OCIO Memorandum, “Contractor Systems,” September 30, 2013:** The OCIO contractor systems memorandum provides a clear definition of each type of contractor system and provides clarification to bureaus that all contractor systems must also obtain authority to operate through the A&A process.

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