



Audit of NARA's Controls over the Use of Information Technology
Equipment and Resources


June 14, 2021

OIG Audit Report No. 21-AUD-08



June 14, 2021

TO: David S. Ferrerio
Archivist of the United States

FROM: Dr. Brett M. Baker 
Acting Inspector General

SUBJECT: *Audit of NARA's Controls over the Use of Information Technology Equipment and Resources* (OIG Audit Report No. 21-AUD-08)

Attached is the final report for the *Audit of NARA's Controls over the Use of Information Technology Equipment and Resources*. We have incorporated the formal comments provided by your office.

As with all OIG products, we determine what information is publicly posted on our website from the attached report. Consistent with our responsibility under the *Inspector General Act, as amended*, we may provide copies of our report to congressional committees with oversight responsibility over NARA.

We appreciate the cooperation and assistance NARA extended to us during the audit. Please contact Jewel Butler, Assistant Inspector General for Audits, with any questions.

Attachment

cc: Debra Wall, Deputy Archivist of the United States
Micah Cheatham, Chief of Management and Administration
William J. Bosanko, Chief Operating Officer
Chris Naylor, Deputy Chief Operating Officer
Swarnali Haldar, Chief Information Officer
Sheena Burrell, Deputy Chief Information Officer
Valorie Findlater, Acting Chief Human Capital Officer
Gary Stern, General Counsel
Neil Carmichael, Director, Insider Threat Program
Kimm Richards, Accountability
Jewel Butler, Assistant Inspector General for Audits
Kimberly Boykin, Audit Director
William Brown, Senior Program Auditor
United States House Committee on Oversight and Government Reform
Senate Homeland Security and Governmental Affairs Committee

Table of Contents

Executive Summary 4

Summary of Recommendations..... 5

Background..... 6

Objective, Scope, Methodology..... 7

Audit Results 10

 Finding 1. An Interdisciplinary Team to Review Inappropriate Internet Use was Ineffective
 10

 Recommendations.....12

 Finding 2. Weaknesses Were Identified in Monthly Inappropriate Use Reports and
 Underlying Data.....14

 Recommendations.....15

 Finding 3. Mobile Device Controls Were Not Implemented18

 Recommendations.....18

Appendix A – Acronyms 20

Appendix B – Prior Audit Recommendations..... 21

Appendix C – Management Response 22

Appendix D – Report Distribution List 26

Executive Summary

Audit of NARA's Controls over the Use of Information Technology Equipment and Resources

OIG Audit Report No. 21 AUD 08

June 14, 2021

Why Did We Conduct This Audit?

The National Archives and Records Administration's (NARA) Directive 802, *Use and Monitoring of NARA Office and Information Technology (IT) Equipment and Resources* (NARA 802), defines appropriate use of NARA IT equipment and resources and staff consent when using NARA's information systems.

The Office of Inspector General (OIG) conducted this audit to determine if controls were adequate and effective to prevent and deter inappropriate use of the Internet on the government-assigned computing resources and mobile devices.

What Did We Recommend?

We made nine recommendations to ensure NARA has proper controls in place to prevent, deter, and detect inappropriate internet use on NARA IT equipment. Management concurred with the recommendations in this report, and in response, provided a summary of their proposed actions.

What Did We Find?

In 2011, the OIG reported weaknesses in NARA's controls over monitoring and preventing inappropriate Internet use by its staff (*Audit of the Controls over Inappropriate Personal Use of the Internet at NARA*, OIG Audit Report No. 11-10, dated March 9, 2011). Although NARA has since made some improvements, examples of internal control deficiencies around inappropriate Internet use continues to exist. We found although NARA has established an informal interdisciplinary team to identify inappropriate Internet use and address potential violations of NARA 802, NARA did not fully comply with the requirements documented in NARA 802, and the team was found to be ineffective due to a lack of management prioritization and ownership of the monitoring of inappropriate internet use. As a result, no office has responsibility for the effective and efficient management and oversight of NARA's inappropriate Internet use.

Additionally, we found monthly inappropriate use reports and underlying data contained incomplete and inaccurate information. The Office of Information Services did not implement sufficient internal controls for the generation, review, and analysis of the monthly inappropriate use reports. Incomplete and inaccurate reports and underlying data to stakeholders hinder NARA's ability to determine: (1) the magnitude of inappropriate use cases; (2) the impact inappropriate use have on NARA IT resources; (3) potential time and attendance fraud; and (4) provide sufficient information to assist further analysis and investigation.

Further, against its policy, NARA mobile devices do not display a user consent banner notifying the user of no expectation of privacy. NARA currently lacks the technical controls to enforce the policy. Without the consent banner, users may try to claim false expectations that the use of assigned mobile devices is private and secure. Also, NARA may have missed opportunities to detect and deter inappropriate use of mobile devices.

Summary of Recommendations

Finding 1: An Interdisciplinary Team to Review Inappropriate Internet Use Was Ineffective

Number	Recommendation	Responsible Office
1	Designate an office to take the ownership of NARA's inappropriate use program, and formally document and communicate to all stakeholders their management and oversight responsibilities for detecting and reporting suspected inappropriate use.	Chief of Management and Administration
2	Update Supplement 1 to NARA Directive 363, <i>NARA Penalty Guide</i> , to include penalties for misusing government IT equipment and resources.	Chief of Management and Administration
3	Retain a complete and centralized work history of technical actions taken when malware or other compromise is the suspected cause of indicators of inappropriate use.	Chief Information Officer

Finding 2: Weaknesses Were Identified in Monthly Inappropriate Use Reports and Underlying Data

Number	Recommendation	Responsible Office
4	Strengthen contract oversight controls to ensure all contract deliverables are completed in a complete, accurate, and timely manner, as it relates to the analyzing and monitoring of inappropriate Internet use on NARA IT resources.	Chief Information Officer
5	Increase the Analytics log retention period in FortiAnalyzer to one year in accordance with NARA Enterprise Architecture.	Chief Information Officer
6	Ensure a process is developed to retrieve IT devices and review user Internet activity on NARA-issued IT devices when they were not connected to NARANet, when other indicators of inappropriate use are detected.	Chief Information Officer
7	Ensure a process is developed to select sample inappropriate use occurrences on a periodic basis for further investigation and analysis.	Chief of Management and Administration

Finding 3: Mobile Device Controls Were Not Implemented

Number	Recommendation	Responsible Office
8	Implement a user consent banner in accordance with NARA Directive 802 on all NARA mobile devices.	Chief Information Officer
9	Disable private browsing on all NARA mobile devices.	Chief Information Officer

Background

National Archives and Records Administration (NARA) Directive 802, *Use and Monitoring of NARA Office and Information Technology (IT) Equipment and Resources* (NARA 802), defines appropriate use of NARA IT equipment and resources and consent for those using NARA's information systems, NARA equipment, or network resources. The policy applies to anyone who uses NARA office or IT equipment or resources including the government-issued desktop, laptop, and tablet computers, and smartphones. The policy states the user does not have a right to, and should not expect, privacy while using any NARA office IT equipment, information system, or resources at any time, including when accessing the Internet or using email.

Various laws and regulations govern the use of government property by the employees and the monitoring of such uses. 5 Code of Federal Regulations (C.F.R) Part 2635, *Standards of Ethical Conduct for Employees of the Executive Branch*, Subpart G contains provisions designed to ensure employees do not misuse their official positions, including an affirmative duty to protect the conserve Government property and to use Government property only for authorized purposes; and a prohibition against using official time other than in an honest effort to perform official duties and a prohibition against encouraging or requesting a subordinate to use official time to perform unauthorized activities. In addition, 18 United States Code (U.S.C.) § 2511 provides legal authority to monitor and intercept communications under prior consent by one of the parties to the communication.

In March 2011, NARA's Office of Inspector General (OIG) issued an audit report¹ on the controls over inappropriate personal use of the Internet, which found controls were inadequate and that NARA employees could access prohibited material by bypassing the web filter. NARA also allowed excessive personal and inappropriate use to go undetected and unaddressed. As a result of the audit, NARA OIG made five recommendations to more thoroughly ensure NARA Directive 802 was enforced. All recommendations from the previous audit are closed.

The estimated program cost for preventing, deterring, monitoring, and taking administrative or personnel action on inappropriate Internet use by NARA staff was \$85,256 in Fiscal Year (FY) 2019 and \$68,579 in FY 2020. NARA has not established a separate program cost for the inappropriate use program; therefore, the cost was estimated based on the hourly rates of the federal and contractor employees who generate or review the monthly inappropriate use reports and produce and perform quality control, and the cost of upgrading NARA's network monitoring and log management tool, provided as part of the Managed Trusted Internet Protocol Services (MTIPS).

¹ Audit of the Controls over Inappropriate Personal Use of the Internet at NARA, OIG Audit Report No. 11-10, dated March 9, 2011.

Objective, Scope, Methodology

Objective

The objective of the audit was to determine whether controls were adequate and effective to prevent and deter inappropriate use of the Internet on the government-assigned computing resources and mobile devices, as defined by NARA 802.

Scope and Methodology

To accomplish our audit objective, we performed audit procedures at Archives II in College Park, Maryland, and from the auditors' approved COVID-19 public health emergency telework location, from January 2020 to March 2021.

Specifically, we performed the following:

- Reviewed applicable laws, regulations, standards, and NARA policies and procedures concerning preventing, deterring, and detecting inappropriate Internet use on NARA IT equipment and resources.
- Conducted interviews with NARA employees and senior executives from the Offices of Human Capital (H), Information Services (I), General Counsel (NGC), and Chief Operating Officer (C), to understand NARA's process for managing and monitoring Internet use on NARA IT equipment and resources.
- Assessed the internal controls around the use of NARA IT equipment and resources to determine if the controls were sufficient to ensure NARA can effectively prevent and deter inappropriate use of the Internet.
- Reviewed nine contractor-generated monthly inappropriate use reports covering the period of April 2019 through January 2020 and associated contract documentation to determine the accuracy, completeness, and sufficiency of the information contained in the reports based on the contract requirements.
- Reviewed 16 complaint referrals made by OIG Office of Investigations (OIG – OI), dated between July and September 2019, and a Management Report titled “*Inappropriate Use Report Vulnerabilities*”, dated February 2020 (NARA-IT-20-0120-S), related to inappropriate Internet use by NARA staff and deficiencies found in the monthly inappropriate use reports.

Additionally, we selected a judgmental sample of 16 NARANet users out of 349 who were included in the monthly inappropriate use reports to further analyze the frequency of violations and remedial or administrative actions taken if necessary. We selected the sample to include the users who were previously reported on the OIG – OI referrals regarding inappropriate Internet use, repeatedly appeared on at least two monthly inappropriate use reports, and had high

numbers of inappropriate use occurrences in the monthly reports reviewed. Various categories of inappropriate Internet use was associated with the users in the sample, including gambling, pornography, proxy avoidance, streaming media and download, and accessing personal social media sites. However, due to a lack of analytics data for the inappropriate use cases in the scope, further analyses on these cases could not be conducted.²

To assess internal controls relative to our objective, we reviewed the Assurance Statements and Internal Control Program (ICP) reports for the Offices of Information Services (I), Human Capital (H), and General Counsel (NGC) for FY 2019 and the first quarter of FY 2020. Information Services submitted a qualified statement of assurance for FY 2019 and FY 2020, reporting on the awareness of the material weakness in internal controls over IT security. Human Capital issued a modified statement of assurance for FY 2019, due to a continuing material weakness in Human Capital declared in September 2018. Information Security and Human Capital remain material weaknesses as of September 2020. General Counsel submitted a statement of full assurance for FY 2019, stating that there is reasonable assurance that the management controls for NGC in effect were adequate and effective. However, General Counsel's ICP report does not specifically address internal controls for responding to inappropriate Internet use by NARA staff.

We assessed the control environment in accordance with the Government Accountability Office's (GAO's) *Standards for Internal Control in the Federal Government* and found management has not effectively established or maintained internal controls to prevent and deter inappropriate use of the Internet on the government-assigned computing resources and mobile devices, as defined by NARA 802. Management did not formally designate, document, or communicate the ownership of the inappropriate use program, resulting in internal control deficiencies in many areas including: (1) deterring users from misusing government IT equipment and resources; (2) ensuring proper administrative or personnel action is taken in response to policy violations; and (3) inappropriate Internet use is consistently detected, logged, and reported.

In planning and performing our audit, we identified the following internal control components and underlying internal control principles as significant to the audit objective: Control Environment, Risk Assessment, Control Activities, Information and Communication, Monitoring, Demonstrate Commitment to Integrity and Ethical Values, Exercise Oversight Responsibility, Establish Structure, Responsibility, and Authority, Demonstrate Commitment to Competence, Enforce Accountability, Assess Fraud Risk, Design Control Activities, Design Activities for the Information System, Implement Control activities, Use Quality Information, Communicate Internally, Perform Monitoring Activities, and Remediate Deficiencies. We assessed the design, implementation, and operating effectiveness of these internal controls and

² Issues related to data storage and availability are discussed in Finding 2, page 12.

identified deficiencies that we believe could affect NARA's ability to ensure inappropriate Internet use is prevented, deterred, and monitored effectively and efficiently. The internal control deficiencies we found are discussed in the Audit Results section of this report. However, because our review was limited to aspects of these internal control components and underlying principles, it may not have disclosed all internal control deficiencies that may have existed at the time of this audit.

This performance audit was conducted in accordance with *Generally Accepted Government Auditing Standards*. Those standards require 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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Kimberly Boykin, Audit Director, Jina Lee, (Lead) Senior IT Auditor, William Brown, Senior Program Auditor, and Kurt Thompson, (Independent Referencer) Senior Program Auditor, made key contributions to this report.

Audit Results

In 2011, the OIG reported weaknesses in NARA's controls over monitoring and preventing inappropriate Internet use by its staff.³ Although NARA has since made some improvements, internal control deficiencies around inappropriate Internet use continues to exist. We found controls were not adequate and effective to prevent and deter inappropriate use of the Internet on the government-assigned computing resources and mobile devices, as defined by NARA 802. Specifically, (1) an interdisciplinary team to review inappropriate internet use was ineffective; (2) weaknesses were identified in monthly inappropriate use reports and underlying data; and (3) mobile device controls were not implemented. As a result, NARA's ability to monitor, track, and report inappropriate use of the Internet by the users remains questionable. For example, in 2017, NARA OIG notified the Chief Information Officer (CIO) that users of the Chrome and Firefox browsers could enable an "Incognito" mode, or "private browsing", which allowed users to browse the Internet without leaving histories. Users were also allowed to delete their browsing histories. These settings created barriers for OIG's investigations into the agency computer misuse.⁴ In addition, NARA has recently received an elevated number of alerts from the Department of Homeland Security (DHS)'s Einstein intrusion detection and prevention system related to malicious video sites that are either hosting inappropriate content or violating copyright laws. These sites were accessed by NARA employees who have access to significant amount of Personally Identifiable Information (PII) that were sometimes found to reside alongside the inappropriately downloaded content. These examples indicate NARA may still be challenged with appropriately mitigating the risks previously identified, in addition to the risk of PII spillage to unauthorized third parties.

Finding 1. An Interdisciplinary Team to Review Inappropriate Internet Use was Ineffective

We found although NARA has established an informal interdisciplinary team to identify inappropriate Internet use and address potential violations of NARA 802, NARA did not fully comply with the requirements documented in NARA 802, and the team was found to be ineffective due to a lack of management prioritization and ownership of the monitoring of inappropriate internet use.

The Office of Management and Budget (OMB) Circular A-123 states management is responsible for establishing and maintaining internal controls to achieve specific internal control objectives

³ Audit of the Controls over Inappropriate Personal Use of the Internet at NARA, OIG Audit Report No. 11-10, dated March 9, 2011.

⁴ The options to enable the Incognito mode have since been disabled on NARA desktop and laptop computers.

related to operations, reporting, and compliance. In addition, GAO's *Standards for Internal Control in the Federal Government* states management acts as necessary to address any deviations from the established policies. As a result of the lack of management prioritization and ownership, no office has responsibility for the effective and efficient management of NARA's inappropriate Internet use. Without proper management and oversight, there is an increased risk that compromised IT resources may go undetected and unresolved. Additionally, users who have violated NARA Directive 802 may remain undetected, and therefore undisciplined.

Ineffective Interdisciplinary Review Team

NARA 802 requires an interdisciplinary review team to identify inappropriate Internet use and address potential violations of NARA 802. The team should meet on a regular basis to review NARA Internet use reports and recommend, as appropriate, further agency action including, but not limited to, initiation of a more-detailed investigation into a particular employee's computer use, re-baselining computer hardware, and consideration of disciplinary action.

In absence of a formal team, in early FY 2020, a group of NARA representatives from various offices⁵ started meeting to review, investigate, and take action upon inappropriate Internet use. However, because this team was informal, it met irregularly and lacked documented policies and procedures to guide its actions. This team is also not functioning as intended by NARA 802.

Additionally, there is no executive ownership of the Inappropriate Use Program, nor is there a designated office that reviews and analyzes the monthly inappropriate use reports (see Finding 2 for further discussion of the reports). Although an Information Services' contractor is responsible for generating the monthly inappropriate use reports, Information Services does not conduct routine review or analysis of the contractor-generated monthly inappropriate use reports. The report is only reviewed by Information Services when a compromise is suspected on a user's machine or NARA's network environment.

The lack of ownership and the informal and decentralized process of reviewing, analyzing, and investigating inappropriate user activity resulted in insufficient analysis of potential threats or abuse. Additionally, data and work history that could have been utilized to determine and perform necessary follow-up actions was insufficient. For example, there were at least five OIG – OI referrals for which management stated malware was suspected on the users' machines; however, no further action was taken to assess, confirm, and remove suspected malware.

⁵ Offices of Human Capital (H), Information Services (I), General Counsel (NGC), Chief Operation Officer – Insider Threat Program (C), and the Office of Inspector General – Office of Investigations (OIG – OI).

No Administrative or Remedial Actions

Although monthly inappropriate use reports identify potential violations of NARA 802, there have not been any personnel actions taken on NARA employees for inappropriate Internet use since at least 2017. During the scope of the audit, the only administrative action taken to address inappropriate Internet use was to issue a NARA-wide communication in October 2019 to reiterate what is prohibited under NARA 802. The communication was issued as a response to a large number of users accessing web sites to stream or download videos, which resulted in an elevated number of alerts from DHS' Einstein 3A intrusion detection and prevention system. Although the web sites accessed oftentimes trick users to download malware onto their machines, NARA did not correlate the alerts to specific individuals, and no further investigation or administrative action at an individual level took place. Additionally, NARA has not included penalties for inappropriate Internet use in Supplement 1 to NARA Directive 363, *NARA Penalty Guide*, which hinders NARA's ability to take disciplinary action in a consistent manner.

Recommendations

We recommend the Chief of Management and Administration:

Recommendation 1: Designate an office to take the ownership of NARA's inappropriate use program, and formally document and communicate to all stakeholders their management and oversight responsibilities for detecting and reporting suspected inappropriate use.

Management Response

NARA will issue an update to NARA Directive 802 that designates an office that is responsible for the inappropriate use program. The policy directive will formally document and communicate responsibilities.

Target Completion Date: September 30, 2021

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 2: Update Supplement 1 to NARA Directive 363, *NARA Penalty Guide*, to include penalties for misusing government IT equipment and resources.

Management Response

NARA will update the penalty guide to assign specific penalties for misusing government IT equipment and resources.

Target Completion Date: September 30, 2021

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

We recommend the Chief Information Officer:

Recommendation 3: Retain a complete and centralized work history of technical actions taken when malware or other compromise is the suspected cause of indicators of inappropriate use.

Management Response

The Cyber Security & Information Assurance Division and Service Operations Delivery Division use an incident handling process for managing security tickets and open investigations. This process creates and stores the work history of technical actions in the ServiceNow system. As evidence of implementation, Information Services will provide work history reports of technical actions taken when malware or other compromise is the suspected cause of indicators of inappropriate use.

Target Completion Date: October 31, 2021

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Finding 2. Weaknesses Were Identified in Monthly Inappropriate Use Reports and Underlying Data

The monthly inappropriate use reports and underlying data contained incomplete and inaccurate information. The reports did not effectively identify inappropriate Internet use and the associated users, or provide sufficient information to assist further analysis and investigation. This occurred because the Office of Information Services did not implement sufficient internal controls for the generation, review, and analysis of the monthly inappropriate use reports. Specifically, Information Services did not: (1) proactively identify and mitigate weaknesses associated with the reports and underlying data; and (2) ensure the reports are reviewed for completeness and accuracy before they were submitted to stakeholders.

NARA Cybersecurity Framework Methodology (CFM) states the agency integrates the analysis of vulnerability scan results, performance data, and network monitoring and system audit log information to monitor information system security status and identify inappropriate or unusual activity at the system level. In addition, NARA Enterprise Architecture requires the Office of Information Services to review and analyze information system audit logs at least on a weekly basis for indications of inappropriate or unusual activity and report findings to designated NARA officials. It also requires NARA retain audit records for a minimum of one year for unclassified information. Incomplete and inaccurate reports and underlying data to stakeholders hinder NARA's ability to determine: (1) the magnitude of inappropriate use cases; (2) the impact they have on NARA IT resources; (3) potential time and attendance fraud; and (4) provide sufficient information to assist further analysis and investigation.

Based on a review of the nine monthly inappropriate use reports and the 16 referrals made by the OIG – OI, we identified weaknesses related to the generation, scope, and review of the reports; and accuracy, sufficiency, storage, and availability of data in the reports.

- Report Generation – Information Services employees were not knowledgeable about generating the report. Instead a NARA Information Technology and Telecommunication Support Services (NITTSS) contractor employee generated the reports. When the employee departed in March 2020, Information Services was unable to generate the report for at least two months, resulting in the contract deliverables being missed. NARA was unable to determine and recover the cost of the missed deliverables from the contractor.
- Report Scope – The reports do not always include the user's NARANet ID or machine name (NARA asset tag) for each inappropriate use occurrence. In such cases, the Internet Protocol (I.P.) address is the only attribute that could potentially be used to associate the activity to a user. However, since NARA utilizes dynamic I.P. addresses instead of static, users' I.P. addresses do not remain consistent, and identifying the user based on the I.P. address is ineffective. In addition, the reports only include use data for the devices

connected to NARANet, either physically or virtually. NARA does not currently have a separate process to review or analyze user activity on the devices when not connected to NARANet. Users may access inappropriate web sites on NARA-issued devices while not connected to NARANet and remain undetected and unmonitored.

- **Report Review** – Although the Performance Work Statement (PWS) for the NITTSS contracts states NARA selects sample incidents for the contractor to investigate for inappropriate user activity, no government personnel have been routinely selecting samples from the monthly inappropriate use reports, besides the referrals made by OIG. In addition, the weekly review of audit logs for indications of inappropriate or unusual activity does not take place as required by NARA Enterprise Architecture.
- **Data Accuracy** – Human errors including incorrect formulas and totals for inappropriate use occurrences were noted in the reports, resulting in inaccurate summary information for the Top 20 users who appeared on the reports the most.
- **Data Sufficiency** – None of the 16 OIG - OI referrals resulted in administrative action because the data contained in the reports was insufficient to conduct thorough and in-depth analysis of user activity. Information Services could not always assist with the level of analysis required to obtain sufficient evidence to determine inappropriate use cases.
- **Data Storage and Availability** – NARA generates the monthly inappropriate use reports based on the user activity data available on the Analytics data storage on FortiAnalyzer.⁶ However, the storage was configured to store approximately only 160 days of user activity. The Archive data, which is off line and cannot be used to generate reports in FortiAnalyzer, was configured to store approximately 464 days of user activity. The misallocation of storage space resulted in the inability to perform analysis or generate reports retroactively once the user activity has passed approximately 160 days. The Office of Information Services recently reallocated the storage space after OIG brought this to its attention. The Analytics data can now be stored for additional days, still less than one year, as required by NARA Enterprise Architecture.

Recommendations

We recommend the Chief Information Officer:

Recommendation 4: Strengthen contract oversight controls to ensure all contract deliverables are completed in a complete, accurate, and timely manner, as it relates to the analyzing and monitoring of inappropriate Internet use on NARA IT resources.

Management Response

Information Services will ensure there is an assigned Government Technical Monitor for contract task orders to conduct performance monitoring. The Contracting Officer's

⁶ A network monitoring and log management tool provided to NARA as part of the MTIPS contract.

Representative will ensure compliance in service delivery. The NARA Information Technology and Telecommunication and Support Services (NITTSS) contract will be updated to expand the language on monitoring of inappropriate use and responsibilities of NARA IT resources.

Target Completion Date: October 31, 2021

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 5: Increase the Analytics log retention period in FortiAnalyzer to one year in accordance with NARA Enterprise Architecture.

Management Response

Information Services has increased the Analytics log retention period to 12 months in FortiAnalyzer and will retain audit records as required by NARA Enterprise Architecture.

Target Completion Date: October 31, 2021

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 6: Ensure a process is to retrieve IT devices and review user Internet activity on NARA-issued IT devices when they were not connected to NARANet, when other indicators of inappropriate use are detected.

Management Response

Information Services' Cybersecurity and Information Assurance Division will update the incident handling procedures to ensure a review of Internet activity when a possible security compromise or malicious activity is detected.

Target Completion Date: August 31, 2021

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

We recommend the Chief of Management and Administration:

Recommendation 7: Ensure a process is developed to select sample inappropriate use occurrences on a periodic basis for further investigation and analysis.

Management Response

NARA will issue an update to NARA Directive 802 (see recommendation 1) that includes a process to periodically select sample inappropriate use occurrences for further investigation and analysis.

Target Completion Date: September 30, 2021

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Finding 3. Mobile Device Controls Were Not Implemented

NARA mobile devices do not display a user consent banner reminding users of no expectation of privacy at log in. Although NARA was previously aware of this issue, addressing it was not a management priority.

NARA 802 indicates the NARANet banner is displayed each time a user logs on to NARANet as a reminder that any use of NARA IT resources is made with the understanding that such use is generally not secure, is not private, and is not anonymous. NARA currently does not have a technical solution to deploy the banner onto mobile devices. Google Mobile Device Management (MDM), a tool NARA utilizes to centrally manage mobile device configurations does not have the feature to deploy the banner. As an alternative, NARA planned to deploy a physical sticker displaying a modified consent banner to all mobile devices in FY 2019. However, as of date, the deployment of the stickers has not been completed.

In addition, private browsing has not been disabled on mobile devices, allowing users to hide or delete browsing history on their devices. NARA 802 states by using NARA IT resources, including mobile devices, users should not expect privacy and no NARA staff have the ability to change this policy or allow any user to expect privacy. Although we found that NARA could disable the private browsing option through the Google MDM, it has not implemented the necessary technical controls to systematically enforce the policy on its mobile devices. Without the consent banner, users may attempt to claim they have false expectations that the use of assigned mobile devices is private and secure. Also, without disabling private browsing, NARA may have missed opportunities to detect and deter inappropriate use of mobile devices.

Recommendations

We recommend the Chief Information Officer:

Recommendation 8: Implement a user consent banner in accordance with NARA Directive 802 on all NARA mobile devices.

Management Response

Information Services is not aware of a technical solution for deploying and displaying an electronic user consent banner within the current MDM environment. Information Services will update the User Consent Form and place a user consent banner sticker on all newly issued mobile devices. In addition, as current devices become eligible for an upgrade, Information Services will apply the sticker to new devices and have the users sign the updated User Consent Form.

Target Completion Date: November 30, 2022

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 9: Disable private browsing on all NARA mobile devices.

Management Response

Information Services is working with SAIC to disable private browsing on all mobile devices.

Target Completion Date: July 31, 2021

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Appendix A – Acronyms

CFM	Cybersecurity Framework Methodology
C.F.R.	Code of Federal Regulations
DHS	Department for Homeland Security
FY	Fiscal Year
GAO	Government Accountability Office
ICP	Internal Control Program
I.P.	Internet Protocol
IT	Information Technology
MDM	Mobile Device Management
MTIPS	Managed Trusted Internet Protocol Services
NARA	National Archives and Records Administration
NITTSS	NARA Information Technology and Telecommunications Support Services
OI	Office of Investigations
OIG	Office of Inspector General
OMB	Office of Management and Budget
PWS	Performance Work Statement
U.S.C.	United States Code

Appendix B – Prior Audit Recommendations

The status of the recommendations from the *Audit of the Controls over Inappropriate Personal Use of the Internet at NARA*, OIG Audit Report No. 11-10, dated March 9, 2011.

Rec. No.	Recommendation Text	Status
1	a. Develop an interdisciplinary team equipped to identify inappropriate use and address violations of NARA Directive 802 with suitable administrative action. b. Establish a threshold of blocked attempts by individual users warranting further analysis for each NARA Directive 802 category. c. Develop a monthly report format containing all the user activity for the NARA staff that surpasses the established blocked attempt thresholds. d. Define formal roles and responsibilities in monitoring and analyzing the reports generated. e. Establish formal criteria based on blocked attempts and successful access totals used to determine if supervisor notification and administrative action is appropriate.	Closed
2	Provide notice to NARA staff that NA and NH are aware of web filter bypass methods in use and focus will be directed toward identifying violators and aggressively pursuing disciplinary action, up to and including removal.	Closed
3	Work with the Websense contract staff on a regular basis to implement all available web filter application features and tools that assist with monitoring and enforcing staff Internet usage in accordance with NARA Directive 802. These include, but are not limited to: a. Generating a customized report identifying NARA users frequenting proxy avoidance websites and analyzing the user activity to determine the extent of inappropriate usage. b. Establishing keyword blocks based on inappropriate weblogs accessed; these keyword blocks should be used to limit what blogs are accessible to NARA employees. c. Determining the feasibility of real-time alerts in relaying inappropriate NARA staff internet usage to NA in order to provide the information in a timely manner. d. Determining the feasibility of quota limits and time period features limiting the amount of time NARA staff can access non-work related websites throughout the workday.	Closed
4	Develop a formal schedule to test Websense for intermittent failures and develop procedures for ensuring the web filtering application is reliable.	Closed
5	Establish tests and procedures to ensure the Websense application at NARA field locations are uniformly configured and no systems are bypassing the web filter.	Closed

Appendix C – Management Response



Date: June 9, 2021
To: Dr. Brett M. Baker, Acting Inspector General
From: David S. Ferriero, Archivist of the United States
Subject: Action Plan to OIG Formal Draft Report, NARA's Controls over the Use of Information Technology Equipment and Resources

Thank you for the opportunity to provide comments on this final report. We appreciate your willingness to meet and clarify language in the report. We concur with the nine recommendations in this audit, and in response, the attachment provides a summary of our proposed actions. As each recommendation is satisfied, we will provide documentation to your office.

If you have questions about this action plan, please contact Kimm Richards at kimm.richards@nara.gov or by phone at 301-837-1668.



DAVID S. FERRIERO
Archivist of the United States

Attachment

NATIONAL ARCHIVES *and*
RECORDS ADMINISTRATION
8601 ADELPHI ROAD
COLLEGE PARK, MD 20740-6001
www.archives.gov

**Action Plan Response to OIG Report
NARA's Controls over the Use of Information Technology Equipment
and Resources**

Recommendation 1: We recommend the Chief of Management and Administration designate an office to take the ownership of NARA's inappropriate use program, and formally document and communicate to all stakeholders their management and oversight responsibilities for detecting and reporting suspected inappropriate use.

Planned Action: NARA will issue an update to NARA Directive 802 that designates an office that is responsible for the inappropriate use program. The policy directive will formally document and communicate responsibilities.

Target Completion Date: September 30, 2021

Recommendation 2: We recommend the Chief of Management and Administration update Supplement 1 to NARA Directive 363, *NARA Penalty Guide*, to include penalties for misusing government IT equipment and resources.

Planned Action: NARA will update the penalty guide to assign specific penalties for misusing government IT equipment and resources.

Target Completion Date: September 30, 2021

Recommendation 3: We recommend the Chief Information Officer retain a complete and centralized work history of technical actions taken when malware or other compromise is the suspected cause of indicators of inappropriate use.

Planned Action: The Cyber Security & Information Assurance Division and Service Operations Delivery Division use an incident handling process for managing security tickets and open investigations. This process creates and stores the work history of technical actions in the ServiceNow system. As evidence of implementation, Information Services will provide work history reports of technical actions taken when malware or other compromise is the suspected cause of indicators of inappropriate use.

Target Completion Date: October 31, 2021

Recommendation 4: We recommend the Chief Information Officer strengthen contract oversight controls to ensure all contract deliverables are completed in a complete, accurate, and timely manner, as it relates to the analyzing and monitoring of inappropriate Internet use on NARA IT resources.

Planned Action: Information Services will ensure there is an assigned Government Technical Monitor for contract task orders to conduct performance monitoring. The Contracting Officer's Representative will ensure compliance in service delivery. The NARA Information Technology and Telecommunication and Support Services (NITTSS) contract will be updated to expand the language on monitoring of inappropriate use and responsibilities of NARA IT resources.

Target Completion Date: October 31, 2021

Recommendation 5: We recommend the Chief Information Officer increase the Analytics log retention period in FortiAnalyzer to one year in accordance with NARA Enterprise Architecture.

Planned Action: Information Services has increased the Analytics log retention period to 12 months in FortiAnalyzer and will retain audit records as required by NARA Enterprise Architecture.

Target Completion Date: October 31, 2021

Recommendation 6: We recommend the Chief Information Officer ensure a process is developed to retrieve IT devices and review user Internet activity on NARA-issued IT devices when they were not connected to NARANet, when other indicators of inappropriate use are detected.

Planned Action: Information Services' Cybersecurity and Information Assurance Division will update the incident handling procedures to ensure a review of Internet activity when a possible security compromise or malicious activity is detected.

Target Completion Date: August 31, 2021

Recommendation 7: We recommend the Chief of Management and Administration ensure a process is developed to select sample inappropriate use occurrences on a periodic basis for further investigation and analysis.

Planned Action: NARA will issue an update to NARA Directive 802 (see recommendation 1) that includes a process to periodically select sample inappropriate use occurrences for further investigation and analysis.

Target Completion Date: September 30, 2021

Recommendation 8: We recommend the Chief Information Officer implement a user consent banner in accordance with NARA Directive 802 on all NARA mobile devices.

Planned Action: Information Services is not aware of a technical solution for deploying and displaying an electronic user consent banner within the current MDM environment. Information Services will update the User Consent Form and place a user consent banner sticker on all newly issued mobile devices. In addition, as current devices become eligible for an upgrade, Information Services will apply the sticker to new devices and have the users sign the updated User Consent Form.

Target Completion Date: November 30, 2022

Recommendation 9: We recommend the Chief Information Officer disable private browsing on all NARA mobile devices.

Planned Action: Information Services is working with SAIC to disable private browsing on all mobile devices.

Target Completion Date: July 31, 2021

Appendix D – Report Distribution List

Archivist of United States
Deputy Archivist of the United States
Chief of Management and Administration
Chief Operating Officer
Deputy Chief Operating Officer
Chief Information Officer
Deputy Chief Information Officer
Acting Chief Human Capital Officer
General Counsel
Director, Insider Threat Program
Accountability

OIG Hotline

To report fraud, waste, or abuse, please contact us:

Electronically: <https://www.archives.gov/oig/referral-form/index.html>

Telephone: 301-837-3500 (Washington, D.C. Metro Area)
1-800-786-2551 (toll-free and outside the Washington, D.C. metro area)

Mail: IG Hotline
NARA
P.O. Box 1821
Hyattsville, MD 20788-0821