USDA
United States Department of Agriculture

Improper Usage of USDA's Information Technology Resources

Audit Report 50501-0020-12

June 2019

OFFICE OF INSPECTOR GENERAL

Improper Usage of USDA's Information Technology Resources

Audit Report 50501-0020-12

USDA OIG reviewed USDA's controls in place to prevent, detect, and report the improper use of information technology resources by employees and non-Government personnel.

OBJECTIVE

Our objective was to determine whether effective controls were in place to prevent, detect, and report improper usage of USDA IT resources.

REVIEWED

OIG reviewed USDA's internal controls to prevent, detect, and report employees' and non-Government personnel's improper use of IT resources at Department and agency levels. To do so, we identified the four agencies with the highest number of improper usage incidents, then tested each agency's networks, reviewed agency records, and conducted interviews with applicable personnel.

RECOMMENDS

The Office of Human Resources Management and OCIO need to define improper usage and develop and implement a documented process for ensuring all parties are notified of incidents, agencies and staff offices need to track and monitor incidents, and OCIO and Departmental Administration need to ensure contractors and other non-Government employees are held accountable to the same improper usage standards as employees.

WHAT OIG FOUND

The National Institute of Standards and Technology defines improper usage as any incident in which an authorized user violates an organization's acceptable usage policies. While USDA's Agriculture Security Operations Center (ASOC), a part of the Office of the Chief Information Office (OCIO), detects and investigates cases of potential information technology (IT) misuse, USDA agencies' supervisors and human resources (HR) personnel serve as a first line of defense in tracking, addressing, and preventing repeat incidents. However, we found that of 36 IT improper use incidents, 28 (approximately 78 percent) were not referred to agencies' HR officials. Of these 28 incidents, 19 (approximately 68 percent) also were not referred to supervisors for potential action. This occurred because neither USDA nor its agencies have sufficient improper usage policies in place to direct agency personnel on how or when to involve HR and supervisors in the remediation process.

Without guidance clearly communicating roles and responsibilities, instances of IT improper use may go unnoticed or unresolved by key parties in the resolution process. Additionally, without appropriate tracking, repeat offenders may be able to continually misuse USDA IT resources, wasting those resources, and exposing USDA networks to increased risk of malware and other internet-based threats.

OCIO, OHRM and the agencies generally concurred with our recommendations and OIG was able to accept management decision for all six recommendations.

United States Department of Agriculture
Office of Inspector General
Washington, D.C. 20250

DATE: June 27, 2019

AUDIT
NUMBER: 50501-0020-12

TO: Gary Washington
Chief Information Officer
Office of Chief Information Officer
ATTN: Megan Davis

Mary Pletcher
Director
Office of Human Resources Management

Victoria Christiansen
Chief
Forest Service
ATTN: Antoine (Tony) Dixon

Kevin Shea
Administrator
Animal and Plant Health Inspection Service
ATTN: Joan M. Conway

Chavonda Jacobs-Young
Administrator
Agricultural Research Service
ATTN: Lisa Baldus

FROM: Gil H. Harden
Assistant Inspector General for Audit Gil H. Harden

SUBJECT: Improper Usage of USDA's Information Technology Resources

This report presents the results of the subject review. Your written response to the official draft is included in its entirety at the end of the report. We have incorporated excerpts from your response, and the Office of Inspector General's (OIG) position, into the relevant sections of the report. Based on your written response, we are accepting management decision for all six audit recommendations in the report, and no further response to this office is necessary. Please follow your internal agency procedures in forwarding final action correspondence to the Office of the Chief Financial Officer (OCFO).

In accordance with Departmental Regulation 1720-1, final action needs to be taken within 1 year of each management decision to prevent being listed in the Department's annual Agency Financial

Report. For agencies other than the Office of the Chief Financial Officer (OCFO), please follow your internal agency procedures in forwarding final action correspondence to OCFO.

We appreciate the courtesies and cooperation extended to us by members of your staff during our audit fieldwork and subsequent discussions. This report contains publicly available information and will be posted in its entirety to our website (http://www.usda.gov/oig) in the near future.

Table of Contents

Background and Objectives

Background

For several years, USDA has faced challenges in addressing information technology (IT) vulnerabilities. Cited as one of the Department's major vulnerabilities, OIG has identified IT security as a major management challenge for more than 10 years.[1] As of November 1, 2018, USDA had 441,896 endpoints in its network environment.[2] Additionally, roles and responsibilities in detecting, preventing, and correcting instances of IT improper usage are spread between two levels: throughout the Department and within each agency.[3]

In September 2017, OIG's Office of Investigations issued a management alert memo to the Office of the Chief Information Officer (OCIO) entitled *Misuse of the U.S. Department of Agriculture's Information Technology Networks*. The memo highlighted that USDA's IT internal controls do not appear to be effectively blocking access to prohibited websites. The Office of Investigations also noted that, since October 2016, USDA OIG had received 81 referrals from the Agriculture Security Operations Center (ASOC) related to potential improper usage activity. The memo recommended that OCIO assess the current software utilized to monitor USDA's IT systems and evaluate its effectiveness in blocking these prohibited websites. Finally, the Office of Investigations recommended that if the current software was deemed ineffective at blocking access, OCIO should identify and install a more effective software solution.

On June 26, 2018, OIG issued an interim report entitled *Improper Usage of USDA's Information Technology Resources—Interim Report*.[4] The interim report was part of this larger audit project. In the interim report, we identified that USDA and agency controls do not prevent USDA users from improperly using USDA IT resources, nor do they consistently detect inappropriate activity. To facilitate USDA taking immediate action, we included seven recommendations for Departmental action in our interim report. We have reached agreement with OCIO on the corrective actions it plans to take for all seven recommendations.

The National Institute of Standards and Technology (NIST) defines improper usage as any incident in which an authorized user violates an organization's acceptable usage policies.[5, 6]

[1] *USDA Management Challenges*, Aug. 2018 (https://www.usda.gov/oig/webdocs/MgmtChallenges2018.pdf).

[2] An endpoint is a remote computing device that communicates back and forth with a network to which it is connected. Examples of endpoints include: desktops, laptops, smartphones, tablets, servers, and workstations. *Palo Alto Networks: Cyberpedia*, https://www.paloaltonetworks.com/cyberpedia/what-is-an-endpoint (last visited Oct. 30, 2018).

[3] For the purposes of this report, the term "agency" refers to both USDA agencies and staff offices; USDA has 35 agencies and offices.

[4] Audit Report 50501-0020-12(1), *Improper Usage of USDA's Information Technology Resources—Interim Report*, June 2018. Due to the report's sensitive content, the interim report was not publicly released due to concerns about the risk of circumvention of the law. A summary is available on our website. (https://www.usda.gov/oig/webdocs/50501-0020-12(1).pdf).

[5] Excluding attacks resulting from external/removable media, attrition, web, email, or impersonation.

[6] NIST, *Computer Security Incident Handling Guide*, Special Publication 800-61 Revision 2 (Aug. 2012).

USDA has issued various Departmental regulations and Departmental manuals that identify specific, unallowable IT uses. For example, Departmental Manual 3525-002, *Internet Use and Copyright Restriction*, prohibits USDA employees from loading peer-to-peer software on USDA equipment, downloading illegal material, downloading copyrighted material for personal use, and distributing illegally obtained files and software.[7] Departmental Regulation 3300-001, *Telecommunications and Internet Services and Use*, prohibits employees from using internet resources for activities that are inappropriate or offensive to fellow employees or the public (for example, accessing sexually explicit materials, hate speech, and/or remarks ridiculing others based on race, creed, religion, color, gender, handicap, national origin, or sexual orientation).[8] According to Departmental policy and the Code of Federal Regulations (C.F.R.), employees also have a duty to protect and conserve Government property and must not allow Government property to be used for unauthorized purposes.[9, 10] Unless authorized in accordance with law or regulations, employees cannot use official time for other purposes.[11]

As stated before, responsibilities to prevent and address IT improper usage are distributed across USDA and require a collaborative approach. For example, according to USDA policy, OCIO is charged with ensuring a system is established to monitor internet usage by all employees, contractors, subcontractors, grantees, and cooperators using USDA equipment to ensure that they adhere to the policy requirements during the performance of their official duties and while using USDA's IT resources.[12] OCIO establishes procedures for monitoring, measuring, reporting, and enforcing compliance with applicable guidance, and oversees agency and staff office compliance with USDA telecommunications policies and procedures.

OCIO policy is to continuously scan all USDA networks and systems to detect unauthorized activity by employees, contractors, subcontractors, grantees, and cooperators. However, based on issues noted in our interim report, OCIO does not possess the ability to view all network traffic.[13] Additionally, the agency information systems security program manager or designee is responsible for identifying and monitoring policy violations and reporting such incidents to OCIO in accordance with USDA computer incident response procedures.

As outlined by Departmental regulation, ASOC, an office within OCIO, is responsible for reporting all cyber security and personally identifiable information incidents to include improper usage activity. ASOC is responsible for managing USDA incidents by communicating and coordinating cyber security incident management for all systems, assets, and data with internal and external entities.[14] ASOC responsibilities includes informing responsible officials—including OIG and individual agencies—of incidents.

[7] USDA Departmental Manual 3525-002, *Internet Use and Copyright Restriction* (Jul. 15, 2004).

[8] USDA Departmental Regulation 3300-001, *Telecommunications and Internet Services and Use* (Mar. 18, 2016).

[9] USDA Departmental Regulation 3300-001, *Telecommunications and Internet Services and Use* (Mar. 18, 2016).

[10] 5 C.F.R. § 2635.704.

[11] 5 C.F.R. § 2635.705.

[12] USDA Departmental Manual 3525-002, *Internet Use and Copyright Restriction* (Jul. 15, 2004).

[13] Audit Report 50501-0020-12(1), *Improper Usage of USDA's Information Technology Resources—Interim Report*, June 2018.

[14] USDA Departmental Regulation 3505-005, *Cyber Security Incident Management Policy* (Oct. 31, 2013).

The *Departmental Personnel Manual* delegates disciplinary authority to agencies and states that the employing agency will conduct investigations of employee misconduct in accordance with Departmental standards. It further states that agencies are authorized to conduct investigations of possible misconduct by agency employees involving violations of rules, regulations, or law that, even if proved, will not likely result in criminal prosecution.[15] OCIO policy similarly states that unauthorized use incidents not involving pornography are forwarded to the agency for review, appropriate followup, and administrative action. However, pornography incidents should be referred to OIG.[16, 17]

Agencies and staff offices are responsible for developing agency-level directives that identify what constitutes acceptable and unacceptable use of IT resources. Each agency has a designated individual to handle and investigate potential IT improper use. Supervisors also play a direct role in addressing and taking corrective action when improper usage does occur.

Objectives

Our objective was to determine whether effective controls were in place to prevent, detect, and report improper usage of USDA IT resources.

[15] USDA Office of Human Resources Management (OHRM), *Departmental Personnel Manual 751-1 Discipline* (Nov. 17, 1981), https://www.dm.usda.gov/employ/employeerelations/dpm-751-1.htm and USDA-OHRM, *Chapter 751 Discipline, Subchapter 3–Agency Investigations of Employee Misconduct* (last visited Oct. 9, 2018), https://www.dm.usda.gov/ohcm/apsd/DPm751sub3.htm.

[16] USDA Departmental Manual 3525-002, *Internet Use and Copyright Restriction* (Jul. 15, 2004).

[17] Our review of the 42 sampled incidents found that all pornography incidents reviewed were properly referred to OIG, as required.

Section 1: Controls Protecting Against the Improper Use of USDA Information Technology Resources

Finding 1: USDA Needs to Implement Policies for Tracking and Disciplining Improper Usage Offenders

We found that USDA does not consistently track IT improper usage incidents and does not always inform the responsible officials in order to prompt further investigation and corrective action. Of 36 IT improper use incidents, 28 (approximately 78 percent) were not referred to agencies' human resources officials (HR). Of these 28 incidents, 19 (approximately 68 percent) also were not referred to supervisors for potential action. This occurred because neither USDA nor its agencies have sufficient improper usage policies in place to direct agency personnel on how or when to involve HR and supervisors in the remediation process. Without clear, comprehensive guidance, USDA, ASOC, and USDA's agencies may not be fully tracking and monitoring incidents to ensure that corrective actions are consistently carried out. Further, without fully monitoring IT improper use, habitual offenders and other users might improperly use USDA IT resources (including its network and equipment), waste USDA resources, and expose USDA networks to increased risk of malware and other internet-based threats.[18]

USDA is required to report all improper usage incidents to the United States Computer Emergency Readiness Team (US-CERT),[19] which defines improper usage as any incident resulting from an authorized user violating an organization's acceptable usage policies.[20, 21] Each agency and staff office is responsible for implementing this policy and associated procedures within its respective agency or staff office. Agencies are also responsible for ensuring that any agency-specific incident management policies and procedures are complete, up-to-date, and in compliance with NIST and USDA policies and procedures.[22]

IT improper usage incidents should be coordinated by ASOC at a Departmental level, working with the agency to resolve agency-specific incidents. At an agency level, incidents should be handled by each agency's incident management personnel.[23] Additionally, HR staff and the users' supervisors are to handle any incidents that may constitute employee misconduct. According to ASOC, it follows USDA draft guidance, which requires ASOC to refer potential IT improper usage incidents to agencies' incident management personnel for further investigation.[24]

[18] Malware is defined as hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose. NIST, *Computer Security Resource Center*, https://csrc.nist.gov/glossary/term/malware (last visited Nov. 7, 2018).

[19] US-CERT serves as the central reporting point for all Federal information security incidents.

[20] USDA Departmental Regulation 3505-005, *Cyber Security Incident Management Policy* (Oct. 31, 2013).

[21] According to US-CERT, this category excludes the following categories: unknown attack, attrition, an attack executed from a website or web-based application, email/phishing, external/removable media, and impersonation/spoofing.

[22] USDA Departmental Regulation 3505-005, *Cyber Security Incident Management Policy* (Oct. 31, 2013).

[23] USDA Departmental Regulation 3505-005, *Cyber Security Incident Management Policy* (Oct. 31, 2013).

[24] This policy was published after audit fieldwork concluded. USDA Departmental Regulation 3505-005, *Cybersecurity Incident Management* (Nov. 30, 2018).

According to this draft guidance, ASOC's point of contact should be the agency's incident management personnel.[25]

Additionally, USDA's Office of Human Resources Management (OHRM) guidance states that agencies are responsible for investigating possible employee misconduct, such as misuse of Government equipment.[26, 27] According to OHRM, the supervisor plays a primary role in preventing and addressing misconduct.[28] OHRM suggests that in matters of employee misconduct, supervisors should counsel the employees.[29] Additionally, OHRM guidance specifies that supervisors can take corrective action including giving verbal warnings and written admonishments. However, it also notes that, for more formal action, the supervisor should consult with the agency's HR staff.[30]

We found that USDA does not consistently track and discipline improper usage activity by employees, contractors, and other non-USDA personnel. We analyzed 42 of 565 incidents identified as potential improper use by ASOC.[31, 32] ASOC referred the incidents to agencies' incident management personnel, who confirmed that 36 of the 42 incidents were improper use incidents.[33]

Because agencies' roles and responsibilities in addressing IT improper use are divided between incident management personnel, HR, and supervisors, it is crucial that agency incident management personnel notify HR and involve users' supervisors after agencies' incident management personnel have confirmed improper use incidents. Even if the incidents do not rise to a level requiring HR disciplinary action, such as malware incidents, which are often inadvertent, HR and users' supervisors should still be notified in order for them to properly track incidents. We found that only 8 of the 36 (approximately 22 percent) improper usage incidents were referred to HR. Of these: three resulted in disciplinary action;[34] three had no further

[25] The draft guidance defines incident management personnel as personnel who are part of a cybersecurity incident response team, those who manage the cybersecurity incident response team personnel, and potentially other personnel with incident handling responsibilities.

[26] USDA OHRM, Chapter 751, "Discipline," Subchapter 3, "Agency Investigations of Employee Misconduct" (last visited Oct. 9, 2018), https://www.dm.usda.gov/ohcm/apsd/DPm751sub3.htm.

[27] OHRM-Employee Relations, *Employee Discipline*, https://www.dm.usda.gov/employ/employeerelations/discipline.htm (last visited Oct. 17, 2018).

[28] Ibid.

[29] USDA OHRM, *Communicating with Employees*, https://www.dm.usda.gov/employ/employeerelations/comm.htm (last visited Oct. 17, 2018).

[30] USDA OHRM, *Employee Discipline,* https://www.dm.usda.gov/employ/employeerelations/discipline.htm (last visited Oct. 17, 2018).

[31] The 42 incidents consist of: 12 malware incidents, 10 unauthorized software incidents, 7 pornography incidents, 5 unidentified users, 4 copyright infringement incidents, 2 unauthorized access incidents, 1 gambling incident, and 1 peer-to-peer incident.

[32] The 565 incidents included 1 OIG incident; however, the OIG incident was excluded from the scope of our audit and any audit-related testing.

[33] The agencies' incident response teams determined that the remaining six incidents did not involve improper use.

[34] Of the three incidents with corrective action: (1) one FS copyright infringement incident resulted in a 10-day suspension; (2) one FS pornography incident resulted in a written last chance agreement which resulted in a 14-day suspension and notification that any further misconduct occurring within the next 2 years would result in termination of employment; and (3) one ARS pornography incident resulted in a 7-day suspension without pay.

actions taken; and, as of October 29, 2018, the remaining two have unresolved HR investigations in progress.

However, 28 of the 36 incidents (approximately 78 percent) were not referred to HR for potential action, and 19 of the 28 (approximately 68 percent) were not referred to a supervisor, even though agencies determined the incident constituted improper use. These types of incidents included improper usage violations such as pornography viewing, unauthorized software installations, and copyright infringement. These incidents should have been investigated further and tracked by agency management and HR.

Incidents were not properly investigated, tracked, or addressed because neither the Department's nor agencies' policies clearly instructed USDA staff on how to resolve incidents involving potential employee misconduct related to improper usage. Although ASOC refers incidents to incident management personnel in individual agencies, the Department and sampled agency policies do not sufficiently cover all aspects of improper usage and the corrective actions that should be taken to address them. For example, these policies:

- do not define all types of improper use,
- do not require a referral to HR or supervisors,
- do not provide guidance on how to address improper use by contractors and non-Government personnel, and
- do not provide guidance on tracking improper usage incidents for employees, contractors, and non-Government personnel.

As a result, agency incident management personnel did not always know how or when to engage with the HR groups charged with overseeing employee misconduct or applicable supervisors.

Definition of Improper Use

NIST defines improper usage as any incident resulting from an authorized user violating an organization's acceptable usage policies. Additionally, according to NIST's guidance, it is the Department's and agencies' responsibility to develop acceptable usage policies that clearly lay out what activities are and are not allowed. However, we found that USDA does not have a Department-wide acceptable use policy and instead directs personnel towards NIST's guidelines.

We reviewed the 36 incidents and compared Departmental and agency level acceptable use policies to determine if the types of misuse were identified in the policies. Our review determined that for 20 of the 36 incidents (approximately 56 percent), the policies did not cover the improper usage category identified. Without knowing what constituted true IT improper use, agency personnel were unsure of what should require HR intervention.

For example, although individual agencies—including the Forest Service (FS), the Agricultural Research Service (ARS), and the Animal and Plant Health Inspection

Service (APHIS)—have their own policies that identify what constitutes acceptable and unacceptable use, OCIO, as an agency, does not.[35] As a result, improper use is not uniformly defined throughout USDA. Specifically, we noted that none of the agencies we tested define contracting malware as improper use, even though ASOC identifies this as a type of improper use.[36] Without a consistent definition of improper use, it is difficult for ASOC to accurately identify which incidents violate the acceptable use policy.

Because NIST's definition of improper use is any violation of agency policy, it is USDA's responsibility to develop sound policies that consistently delineate and define types of improper use and corrective actions to take. Without adequately defining improper use—and a specific course of action for each type—instances of potential improper use may go uninvestigated, not referred, or unresolved.

Referral of Improper Use Incidents to the Supervisor and HR

Additionally, agency and Departmental guidance and policies did not always require all types of improper use to be referred to HR or supervisors. This inconsistency led to USDA and its agencies inconsistently responding to potential employee misconduct and its related risks.

For example, while ARS requires streaming improper use incidents to be referred to HR, FS and APHIS do not. Similarly, although FS and ARS require copyright infringement and gambling to be referred to HR, APHIS does not. Additionally, neither APHIS, ARS, nor FS required other types of improper usage, such as installing unapproved software, to be referred to HR, even though the agencies identified it as unacceptable. Additionally, OCIO, at an agency level, does not have clear guidance establishing when improper use incidents should be referred to the supervisor or relevant HR unit. Without clear guidance specifying the need for a referral, incidents may be overlooked or may not be appropriately investigated.

Even when policy was in place clarifying what constitutes improper use, we found that it was not always followed. For example, although there were 11 improper usage incidents at ARS in our sample, including incidents of peer-to-peer networking,[37] downloading

[35] APHIS, ARS, and FS all identify pornography, unauthorized software, streaming, and gambling as unacceptable use. Additionally, FS and ARS identify peer-to-peer networking and copyright infringement as unacceptable use, while APHIS does not. Similarly, USDA guidance identifies activities that are inappropriate or offensive to fellow employees or the public as inappropriate use. In addition, it identifies the installation of peer-to-peer software, downloading of illegal material, downloading copyrighted material for personal use, and the distribution of illegally obtained files and software, as inappropriate use. Although these policies list types of improper use, and the types of improper use overlap with other agencies, the types and definition of improper use is not universally defined within USDA.

[36] FS defines intentionally installed malware as improper use.

[37] Peer-to-peer networking involves a group of computers linked together with equal permissions and responsibilities for processing data. Peer-to-peer networking allows for large files to be shared over the internet.

unauthorized software, and copyright infringement, only one incident (a pornography-related incident) was reported to HR.[38]

OHRM policy requires supervisors and HR to work in tandem. Based on a review of the OHRM-Employee Relations webpage*,* supervisors play an important role not only in correcting, but in preventing misconduct, including improper IT usage. If all involved parties do not communicate and coordinate their corrective actions, USDA and its agencies may not be taking consistent, appropriate corrective action. However, we noted that even when agency policies and procedures required HR to be notified, they did not require that the IT users' supervisors (whether employees, contractors, or non-Government personnel) be notified of the improper usage.

For example, one incident was reported to a supervisor, but not HR. The incident involved an OCIO employee's computer, which was used to access pornography. After being informed that an employee's computer accessed pornographic images, the supervisor interviewed the user, who denied visiting any pornographic sites. According to OCIO, the employee's supervisor discussed the incident with the employee, which was considered a verbal warning, but did not take disciplinary action or refer the matter to HR. As a result, no further action was taken.

As this instance illustrates, without coordination between supervisors and HR, incidents may not be thoroughly examined and corrective actions may not be consistently carried out. While this incident resulted in an informal verbal warning, HR action for similar pornography incidents in other agencies have included: (1) a written last-chance agreement for an FS employee, which resulted in a 14-day suspension and employee notification that any further misconduct incidents within the next 2 years would result in termination of employment; (2) a 7-day suspension of an ARS employee without pay; and (3) no action.

Guidance needs to be comprehensive and include clear roles and responsibilities for both HR and supervisors, who should monitor corrective actions to ensure they are consistently carried out. Otherwise, agencies may be taking corrective action without understanding the complete picture—or not taking corrective action at all.

Guidance for Contractors and other Non-Government Personnel

We also noted that the policies and procedures in place within the Department and at the agencies we tested did not provide guidance to contracting officer representatives and sponsors of non-Government personnel on how to address improper use by contractors and other non-Government personnel. For example, we identified 11 improper use incidents that involved contractors, a visiting scientist, or unidentified users.[39] For 9 of

[38] While our sample contained 11 ARS incidents, 4 of these were malware issues. We acknowledge that malware incidents may not rise to the level of HR corrective action, since they often can occur inadvertently.

[39] Unidentified users were individuals (employee, contractor, or non-Government personnel) responsible for the activity that the agency could not identify. Unidentified users also included users on the agency's guest network.

these 11 incidents (approximately 82 percent), no corrective actions were taken. For the remaining two incidents, one contractor installed an unauthorized television streaming application and another viewed pornographic websites. Because guidance is unclear on how to address a contractor's or non-Government personnel's improper usage, we were unable to determine what corrective actions, if any, were taken for these two incidents.[40]

Without USDA guidance on how to address contractor and non-Government personnel improper use, these incidents may not be appropriately tracked or addressed.

Tracking of Improper Use Incidents

We also noted that the policies and procedures in place within the Department and at the agencies do not provide guidance on tracking IT users' incidences of improper use in regard to potential employee, contractor, or non-Government personnel misconduct.[41]

Because guidance does not instruct Departmental and agency personnel to track IT improper use incidents as potential misconduct, USDA and agency-level involved parties—be they OCIO, HR, supervisors, or incident management personnel—did not consistently identify repeat offenders. We found this lack of tracking to be an issue both with USDA employees and contractors working on behalf of USDA. For instance, because of poor tracking, neither OIG nor the agency could determine if the contractor who installed an unauthorized streaming application (mentioned above) received any corrective action.

Similarly, we identified a pornography-related incident committed by a repeat offender. However, the agency's HR had no record of the prior offenses and could not tell us whether these multiple offenses were taken into account when penalties were assessed. Due to inconsistent tracking, we were unable to determine how many repeat offenders existed within the universe of improper usage incidents. Until USDA implements a consistent policy, habitual offenders might not be identified and may therefore continue to improperly use USDA IT resources, including its network and equipment.

When we spoke with OCIO, it acknowledged that there was a problematic lack of overarching written policies and procedures that would: (1) ensure HR and supervisors are involved and aware, and (2) give clear guidance on how to address improper use by contractors and other non-Government personnel.

Without guidance clearly communicating roles and responsibilities, instances of IT improper use may go unnoticed or unresolved by key parties in the resolution process. Additionally, without

[40] The first contractor's site supervisor had retired and other management was no longer managing the contract. The second contractor was terminated due to lack of funding before the incident could be investigated. For these incidents, the agencies could not provide any records documenting a course of disciplinary action for these individuals.

[41] ASOC tracks improper use incidents to ensure that the incident is mitigated by the agency IT staff and reported to US-CERT, as appropriate.

appropriate tracking, repeat offenders may be able to continually misuse USDA's IT resources, wasting those resources and exposing USDA networks to increased risk of malware and other internet-based threats.

Recommendation 1

OHRM, in coordination with OCIO, needs to define improper usage activity and develop and implement a process, documented via policy, for ensuring all parties (supervisors, HR personnel, agencies' IT and incident handling teams) are properly notified of improper usage incidents.

Agency Response

In its June 19, 2019, response, OHRM stated:

> This staff office agrees with this recommendation. OHRM, in coordination with OCIO, will define improper usage activity and develop and implement a process, documented via policy, for ensuring all parties (supervisors, HR personnel, agencies' IT and incident handling teams) are properly notified of improper usage incidents.
>
> September 6, 2019: Define improper usage and develop a process to ensure all parties are properly notified of improper usage incidents.
>
> April 30, 2020: Implement Departmental policy or Departmental memorandum requiring implementation of the improper use process and definitions.

OIG Position

We accept management decision.

Recommendation 2

OCIO, in coordination with Departmental Administration, needs to develop and implement a process, documented via policy, for ensuring contractors and other non-Government employees are held accountable to the same improper usage standards as employees.

Agency Response

In its May 17, 2019, response, OCIO stated:

> OCIO agrees with this Recommendation. The OCIO and OHRM improper usage incident process identified in recommendation 1, will provide guidance so that Federal and non-Federal personnel are held accountable to the same improper usage standards.

> OCIO and/or OHRM will publish a Department policy or Departmental memorandum identifying the improper usage incident process as a Department procedure.
>
> September 6, 2019: Define improper usage, develop and publish the Departmental improper usage process for agency use.
>
> April 30, 2020: Publish Departmental policy or Departmental memorandum identifying the improper use process as Departmental policy.

OIG Position

We accept management decision.

Recommendation 3

ARS needs to implement procedures in accordance with Departmental policies developed in response to Recommendations 1 and 2 to ensure appropriate management officials such as supervisors, contracting officials, and supervisors of non-Government personnel are notified to make sure employees, contractors, or non-Government personnel that engage in improper usage of IT resources are properly tracked and monitored.

Agency Response

In its May 21, 2019, response, ARS stated:

> ARS agrees with this Recommendation. ARS will implement procedures, in accordance with Departmental policies developed in response to Recommendations 1 and 2, to ensure appropriate management officials such as supervisors, contracting officials, and overseers of non-Government personnel are notified to make sure employees, contractors, and non-Government personnel that engage in improper usage of IT resources are properly tracked and monitored. ARS stated that it will implement these procedures no later than April 30, 2010.

OIG Position

We accept management decision.

Recommendation 4

APHIS needs to implement procedures in accordance with Departmental policies developed in response to Recommendations 1 and 2 to ensure appropriate management officials such as supervisors, contracting officials, and supervisors of non-Government personnel are notified to make sure employees, contractors, or non-Government personnel that engage in improper usage of IT resources are properly tracked and monitored.

Agency Response

In its May 22, 2019, response, APHIS stated:

> APHIS agrees with this Recommendation. On May 3, 2019, APHIS … issued a Delegation of Authority Memo within the Agency that clearly identifies who may propose, decide or take specified actions as they relate to these type of situations. APHIS will continue to implement procedures, in accordance with Departmental policies, developed in response to Recommendations 1 and 2, to ensure appropriate management officials such as supervisors, contracting officials, and supervisors of non-Government personnel are notified to make sure employees, contractors, on non-Government personnel that engage in improper usage of IT resources are properly tracked and monitored. APHIS will implement this Recommendation by April 30, 2020.

OIG Position

We accept management decision.

Recommendation 5

FS needs to implement procedures in accordance with Departmental policies developed in response to Recommendations 1 and 2 to ensure appropriate management officials such as supervisors, contracting officials, and supervisors of non-Government personnel are notified to make sure employees, contractors, or non-Government personnel that engage in improper usage of IT resources are properly tracked and monitored.

Agency Response

In its May 16, 2019 response FS stated:

> FS agrees with this recommendation and will implement procedures, in accordance with Departmental policies, developed in response to Recommendations 1 and 2, to ensure appropriate management officials such as supervisors, contracting officials, and supervisors of non-Government personnel are notified to make sure employees, contractors, or non-Government personnel that engage in improper usage of IT resources are properly tracked and monitored.

FS estimates it will implement this recommendation by June 1, 2020.

OIG Position

We accept management decision.

Recommendation 6

OCIO needs to implement procedures in accordance with Departmental policies developed in response to Recommendations 1 and 2 to ensure appropriate management officials such as supervisors, contracting officials, and supervisors of non-Government personnel are notified to make sure employees, contractors, or non-Government personnel that engage in improper usage of IT resources are properly tracked and monitored.

Agency Response

In its May 17, 2019, response, OCIO stated:

> OCIO agrees with this Recommendation. OCIO will update its cybersecurity improper use procedures based upon the OCIO and OHRM improper use definition and the process identified in recommendations 1 and 2. The OCIO procedures will identify when appropriate Federal and non-Federal supervisors are to be notified of incidents of improper usage and require tracking and monitoring of Federal and non-Federal personnel that improperly use IT resources.

OCIO estimates the completion date to be April 30, 2020.

OIG Position

We accept management decision.

Scope and Methodology

As part of this engagement, OIG tested select agencies after analyzing USDA's universe of related incidents. The engagement concentrated on internal controls implemented to prevent, detect, and report employees' and non-Government personnel's improper use of information technology resources at the Department and agency levels for FY 2017 and the first 2 months of FY 2018.

To review the internal controls, we obtained a list of all of USDA's 565 improper usage incidents from ASOC's incident ticketing system for October 1, 2016, through November 30, 2017, which covered all types of improper usage. We then used ACL™ Analytics to analyze the 565 incidents to identify the four agencies with the highest number of improper usage incidents during this period: APHIS, ARS, FS, and OCIO.[42, 43] Our analysis resulted in a universe of a 171 incidents at FS, 121 incidents at ARS, 53 incidents at OCIO, and 48 incidents at APHIS. From those four agencies, we selected a sample of approximately 10 percent of each agency's improper use incidents. Our analysis resulted in a sample size of 18, 13, 6, and 5 incidents, respectively, for a total of 42 incidents.

Once the sample was selected, we reviewed the incident details and categorized the incident into the following categories:

- malware incidents,
- unauthorized software incidents,
- pornography incidents,
- unidentified users,
- copyright infringement incidents,
- unauthorized access incidents,
- gambling incidents, and
- peer-to-peer incidents.

We reviewed the sample incidents to determine whether agencies followed their policy and procedures for taking and documenting appropriate disciplinary action. We assessed the completeness of the universe provided by ASOC by comparing the list of improper use incidents provided by ASOC to the lists of improper use incidents provided by each agency in our sample. For the purposes of this audit, we did not assess the controls surrounding the incident ticketing system, as that assessment was outside the scope of our audit.

We conducted interviews with appropriate personnel at each agency and reviewed relevant Department and agency policies and procedures. Additionally, we obtained personnel records for each incident that resulted in a human resource action. We also collaborated with an OIG

[42] ACL™ Analytics is an application that provides a combination of data access, data analysis, and integrated reporting capabilities.

[43] OIG was excluded from the scope of our audit. Although one incident from OIG was included in our universe, it was not included in our sample or subsequent audit testing.

forensic examiner within OIG's Technical Crimes Division to conduct the testing at each of the four selected agencies. The results of this testing are documented in the interim audit report. Testing at each agency consisted of:

- attempting to access websites for which there is no known business purpose,
- attempting to access websites identified as blocked by agencies and/or the Department;
- installing software for which there is no known business purpose,
- using tools available on the internet to circumvent USDA controls for blocking inappropriate content, and
- attempting to rearrange the boot order of the computer by changing the basic input/output system settings (BIOS), then booting to a universal serial bus (USB) drive.[44]

Fieldwork was performed from December 2017 to November 2018 at offices in Beltsville, Maryland; Riverdale, Maryland; Albuquerque, New Mexico; Washington, D.C.; and Kansas City, Missouri.

We conducted this audit in accordance with Generally Accepted Government Auditing Standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[44] The BIOS software has a number of different roles, but its most important role is to load the operating system. BIOS makes sure all the other chips, hard drives, ports, and central processing unit function together. A bootable USB uses a USB storage device to enable computer hardware to use the device to acquire all essential system booting information and usually bypasses the hard drive, depending on the settings in the BIOS.

Abbreviations

APHIS	Animal and Plant Health Inspection Service
ARS	Agricultural Research Service
ASOC	Agriculture Security Operations Center
C.F.R.	Code of Federal Regulations
FS	Forest Service
HR	human resources
IT	information technology
NIST	National Institute of Standards and Technology
OCIO	Office of Chief Information Officer
OIG	Office of Inspector General
OHRM	Office of Human Resources Management
US-CERT	United States Computer Emergency Readiness Team
USDA	Department of Agriculture

AGENCIES' RESPONSES TO AUDIT REPORT

USDA

United States Department of Agriculture

June 26, 2019

Departmental Administration

Office of the Assistant Secretary for Administration

Office of Human Resources Management

1400 Independence Avenue, SW
Washington, DC
20250-9600

FOR: Gil H. Harden
Assistant Inspector General for Audit
Office of Inspector General

FROM: Mary Pletcher Rice /s/
Chief Human Capital Officer
Office of Human Resources Management

SUBJECT: Audit 50501-0020-12 (Recommendation Response)

The Office of Human Resources Management (OHRM) is requesting Management Decision concurrence on recommendation 1 of the subject audit.

OIG AUDIT RECOMMENDATION 1:
OHRM, in coordination with Office of the Chief Information Officer (OCIO), needs to define improper usage activity and develop and implement a process, documented via policy, for ensuring all parties (supervisors, HR personnel, agencies' IT and incident handling teams) are properly notified of improper usage incidents.

RECOMMENDATION 1 RESPONSE:
This staff office agrees with this recommendation. OHRM, in coordination with OCIO, will define improper usage activity and develop and implement a process, documented via policy, for ensuring all parties (supervisors, HR personnel, agencies' IT and incident handling teams) are properly notified of improper usage incidents.

RECOMMENDATION 1 TIMELINE PROJECTIONS:

- September 6, 2019: Define improper usage and develop a process to ensure all parties are properly notified of improper usage incidents.

- April 30, 2020: Implement Departmental policy or Departmental memorandum requiring implementation of the improper use process and definitions.

Should you have any questions pertaining to this referral, please contact Mr. Kevin McGrath, Branch Chief, Employee and Labor Relations Division, on 202-260-8160 or via email address Kevin.McGrath@usda.gov.

cc:
Gary Washington, Chief Information Officer, OCIO
Dennis Phelan, ASOC, OCIO, Washington, DC

United States Department of Agriculture

Departmental Administration

Office of the Chief Information Officer

1400 Independence
Avenue S.W.
Washington, DC
20250

TO: Gil H. Harden
Assistant Inspector General for Audit
Office of Inspector General

FROM: Gary S. Washington /s/
Chief Information Officer
Office of the Chief Information Officer

SUBJECT: Request for Management Decision Concurrence on Recommendations 2 and 6 of the Office of Inspector General Audit 50501-0020-12 *"Improper Usage of USDA Information Technology Resources"*

The Office of the Chief Information Officer (OCIO) is requesting Management Decision concurrence on recommendations 2 and 6 of the subject audit.

Recommendation 2:
OCIO, in coordination with Departmental Administration, needs to develop and implement a process, documented via policy, for ensuring contractors and other non-Government employees are held accountable to the same improper usage standards as employees.

OCIO Response:
The Department concurs with this recommendation.

Corrective Actions:
OCIO agrees with this Recommendation. The OCIO and OHRM improper usage incident process identified in recommendation 1, will provide guidance so that Federal and non-Federal personnel are held accountable to the same improper usage standards.

OCIO and/or OHRM will publish a Department policy or Departmental memorandum identifying the improper usage incident process as a Department procedure.

Estimated Completion Date:
September 6, 2019: Define improper usage, develop and publish the Departmental improper usage process for agency use.

April 30, 2020: Publish Departmental policy or Departmental memorandum identifying the improper use process as Departmental policy.

Recommendation 6:
OCIO needs to implement procedures in accordance with Departmental policies, developed in response to recommendations 1 and 2, to ensure appropriate management

officials such as supervisors, contracting officials, and supervisors of non-Government personnel are notified to make sure employees, contractors, or non-Government personnel that engage in improper usage of IT resources are properly tracked and monitored.

OCIO Response:
The Department concurs with this recommendation.

OCIO agrees with this Recommendation. OCIO will update its cybersecurity improper use procedures based upon the OCIO and OHRM improper use definition and the process identified in recommendations 1 and 2. The OCIO procedures will identify when appropriate Federal and non-Federal supervisors are to be notified of incidents of improper usage and require tracking and monitoring of Federal and non-Federal personnel that improperly use IT resources.

Estimated Completion Date:
April 30, 2020

We shall continue to keep you posted of our progress on these recommendations.

If additional information is needed, please contact Megen Davis, OCIO Audit Liaison, on telephone number (301) 504-4299 or via email at megen.davis@wdc.usda.gov.

Cc: Venice Goodwine, OCIO, Chief Information Security Officer
Tacy Summersett, OCIO, Deputy Chief Information Security Officer
Mary Pletcher, Office of Human Resources Management, Director
Antoine Dixon, Forest Service, Chief Financial Officer
Amy Faden, Forest Service, Branch Chief
Dan Rodrin, Forest Service, Financial Statement Audit Liaison
Chavonda Jacobs-Young, Agricultural Research Service, Administrator
Kevin Shea, Animal and Plant Health Inspection Service, Administrator
Annie Walker-Bradley, OCFO, Director, Internal Control Division
Lynn Moaney, OCFO, Associate Chief Financial Officer
Lance Moore, OIG, Assistant Regional Inspector General
Tonya Judkins, OCIO Chief of Staff
Megen Davis, OCIO Audit Liaison

USDA
United States Department of Agriculture
Research, Education, and Economics
Agricultural Research Service

May 21, 2019

SUBJECT: Agricultural Research Service's Response
to the Office of Inspector General (OIG) Report,
"Improper Usage of USDA Information Technology Resources"
(50501-0020-12)

TO: Gil H. Harden
Assistant Inspector General for Audit

FROM: Lisa A. Baldus /s/
Associate Deputy Administrator
Administrative and Financial Management
Agricultural Research Service

Thank you for the opportunity for the Agricultural Research Service (ARS) to comment on the Office of Inspector General Report, "Improper Usage of USDA Information Technology Resources". The following is our response and action plan to Recommendation 3.

ARS agrees with this Recommendation. ARS will implement procedures, in accordance with Departmental policies developed in response to Recommendations 1 and 2, to ensure appropriate management officials such as supervisors, contracting officials, and overseers of non-Government personnel are notified to make sure employees, contractors, and non-Government personnel that engage in improper usage of IT resources are properly tracked and monitored. ARS will implement these procedures within 120 days of the official release of the latest of the two Departmental policies or not later than April 30, 2020.

If you have any questions, please contact me at (301) 504-1032 or at Lisa.Baldus@ARS.USDA.GOV.

cc:
C. Jacobs-Young, Administrator

USDA

United States Department of Agriculture

Animal and Plant Health Inspection Service

Washington, DC 20250

MEMORANDUM

TO: Gil H. Harden
Assistant Inspector General for Audit

FROM: Kevin Shea /S/
Administrator
Animal and Plant Health Inspection Service

SUBJECT: Animal and Plant Health Inspection Service's (APHIS) Response and Request for Management Decision on the Office of Inspector General (OIG) Report, "Improper Usage of USDA Information Technology Resources" (50501-20-12)

Thank you for the opportunity for APHIS to comment on this report. We have addressed Recommendation #4.

APHIS believes its agency is working diligently to ensure that effective controls are in place to prevent, detect and report improper usage of the agency's information technology resources. APHIS has invested and developed a robust cybersecurity program that has helped deter agency employees from misuse of the agency's information technology resources. For example, on January 24, 2018, APHIS deployed CheckPoint--a firewall/intrusion prevention system--with automated defenses that prohibit access to internet sites deemed as inappropriate, such as pornographic and gambling. To date, APHIS has implemented over 23 CheckPoint defined categories that prohibit access to sites deemed as improper (i.e., misuse).

In terms of numbers, since 2018, APHIS has blocked nearly 2 billion cybersecurity and IT misuse attempts from entering or leaving our networks. In addition to the automated blocks, APHIS' cybersecurity team has investigated and then blocked over 55 sites and 160 URLs, which have further enhanced the agency's ability to prevent employees from reaching unauthorized sites.

In addition to APHIS employing CheckPoint, since April 2018, APHIS has implemented new agency procedures for the agency's human resources office and the cybersecurity office to collaboratively work on the timely detection and reporting on the misuse of the agency's information technology resources, in regard to agency employees attempting and/or visiting suspected pornographic sites. This information is obtained, reviewed and also reported.

Recommendation 4

APHIS needs to implement procedures in accordance with Departmental policies, developed in response to Recommendations 1 and 2, to ensure appropriate management officials such as supervisors, contracting officials, and supervisors of non-Government personnel are notified to make sure employees, contractors, or non-Government personnel that engage in improper usage of IT resources are properly tracked and monitored.

APHIS Response: APHIS agrees with this Recommendation. On May 3, 2019, APHIS Administrator Kevin Shea issued a Delegation of Authority Memo within the Agency that clearly identifies who may propose, decide or take specified actions as they relate to these type of situations. APHIS will continue to implement procedures, in accordance with Departmental policies, developed in response to Recommendations 1 and 2, to ensure appropriate management officials such as supervisors, contracting officials, and supervisors of non-Government personnel are notified to make sure employees, contractors, on non-Government personnel that engage in improper usage of IT resources are properly tracked and monitored. APHIS will implement this Recommendation by April 30, 2020.

Forest Service

Washington Office

1400 Independence Avenue, SW
Washington, D.C. 20250

File Code:	1430	**Date:**	May 16, 2019
Route To:			

Subject: FS Response to Reach Management Decision on OIG Report No. 50501-0020-12 Improper Usage of USDA Information Technology Resources

To: Gil H. Harden, Assistant Inspector General for Audit, Office of Inspector General

Thank you for the opportunity to review and comment on Office of Inspector General (OIG) Draft Report Number 50501-0020-12. The Forest Service concurs with the findings and recommendations and appreciates the time and effort that went into the report. The agency's response to the Forest Service audit recommendation is enclosed. Please contact Antoine Dixon, Chief Financial Officer, at (202) 205-0429 or antoine.dixon@usda.gov with any questions.

/s/ Victoria Christiansen
VICTORIA CHRISTIANSEN
Chief

Enclosure

==

USDA Forest Service (FS)

==

Office of Inspector General (OIG) Audit Report No. 50501-0020-12
Improper Usage of USDA Information Technology Resources
Official Draft Issued April 18, 2019

Response to the Official Draft Report / Management Decision Request

==

Recommendation 5: FS needs to implement procedures in accordance with Departmental policies, developed in response to Recommendations 1 and 2, to ensure appropriate management officials such as supervisors, contracting officials, and supervisors of non-Government personnel are notified to make sure employees, contractors, or non-Government personnel that engage in improper usage of IT resources are properly tracked and monitored.

Forest Service (FS) Response: FS agrees with this recommendation and will implement procedures, in accordance with Departmental policies, developed in response to Recommendations 1 and 2, to ensure appropriate management officials such as supervisors, contracting officials, and supervisors of non-Government personnel are notified to make sure employees, contractors, or non-Government personnel that engage in improper usage of IT resources are properly tracked and monitored.

Estimated Completion Date: June 1, 2020

Learn more about USDA OIG
Visit our website: www.usda.gov/oig/index.htm
Follow us on Twitter: @OIGUSDA

How to Report Suspected Wrongdoing in USDA Programs

Fraud, Waste, and Abuse
File complaint online: www.usda.gov/oig/hotline.htm

Monday–Friday, 9:00 a.m.– 3:00 p.m. ET
In Washington, DC 202-690-1622
Outside DC 800-424-9121
TDD (Call Collect) 202-690-1202

Bribes or Gratuities
202-720-7257 (24 hours)

All photographs are from USDA's Flickr site and are in the public domain.