TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

The Computer Security Incident Response Center Is Preventing, Detecting, Reporting, and Responding to Incidents, but Improvements Are Needed

August 28, 2017

Reference Number: 2017-20-050

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.

Phone Number / 202-622-6500
E-mail Address / TIGTACommunications@tigta.treas.gov
Website / http://www.treasury.gov/tigta

To report fraud, waste, or abuse, call our toll-free hotline at:

1-800-366-4484

By Web:

www.treasury.gov/tigta/

Or Write:

Treasury Inspector General for Tax Administration
P.O. Box 589
Ben Franklin Station
Washington, D.C. 20044-0589

Information you provide is confidential and you may remain anonymous.

HIGHLIGHTS

THE COMPUTER SECURITY INCIDENT RESPONSE CENTER IS PREVENTING, DETECTING, REPORTING, AND RESPONDING TO INCIDENTS, BUT IMPROVEMENTS ARE NEEDED

Highlights

Final Report issued on August 28, 2017

Highlights of Reference Number: 2017-20-050 to the Internal Revenue Service Chief Information Officer.

IMPACT ON TAXPAYERS

The IRS's Computer Security Incident Response Center (CSIRC) is the office responsible for preventing, detecting, reporting, and responding to cybersecurity incidents, which are computer-related threats or attacks targeting the IRS's enterprise information technology assets. Because the IRS maintains tax information on all taxpayers, the IRS is an attractive target for hackers. Weaknesses in the CSIRC program could prevent the timely detection, prevention, or reporting of unauthorized access and disclosure of taxpayer data.

WHY TIGTA DID THE AUDIT

This audit was initiated to evaluate the CSIRC's effectiveness at preventing, detecting, reporting, and responding to computer security incidents targeting IRS computers and data. In addition, TIGTA followed up on the corrective actions for findings and recommendations from two prior audit reports that involved the CSIRC operations.

WHAT TIGTA FOUND

In general, the CSIRC prevented, detected, reported, and responded to cybersecurity incidents. For example, TIGTA sampled 100 incidents from a total population of 368 incidents for Fiscal Years 2015 and 2016 (through April 30, 2016). The CSIRC properly identified and documented the type, nature, and scope of all 100 incidents with information such as the systems and applications affected, the source of the incident, and the specific kind of lost equipment. However, TIGTA identified the following areas in which the CSIRC could improve its operations.

The CSIRC could improve some aspects of incident case work. TIGTA found that not all incidents were properly reported, some supporting incident documentation was insufficient, incident costs were not captured, and reporting procedures were inconsistently applied. For example, 64 of the 100 incidents were required to be reported to the Department of the Treasury CSIRC because the incidents were confirmed to have compromised the confidentiality, integrity, or availability of a Federal Government information system. Of the 64 incidents, 22 were not reported as required. On February 15, 2017, after bringing the noncompliance to the IRS's attention, the 22 incidents were reported to the Department of the Treasury CSIRC.

CSIRC employees and contractors did not always meet training guidelines, and skill assessments demonstrate a need for more training. Not all CSIRC employees complied with the Federal Information Security Modernization Act and required internal specialized security training for Fiscal Years 2015 and 2016. The employees took courses the IRS deemed as specialized; however, TIGTA disagreed with the designation after a closer review of the courses' objectives. In addition, there was no documentation that contractors met the same requirements for the same periods.

Finally, the Incident Response Plan, which provides the organization with a roadmap for implementing its incident response capability, was developed, but was not updated to fully comply with Federal guidelines.

WHAT TIGTA RECOMMENDED

While the IRS corrected several of the issues prior to completion of this report, TIGTA made five recommendations to the Chief Information Officer. The recommendations were: correcting reporting inconsistencies of incidents, ensuring costs of handling and responding to incidents are captured, ensuring that CSIRC employees and contractors are compliant with the specialized security training requirements, removing contractor access privileges to IRS systems when contractors are noncompliant with training requirements, and ensuring that employee receive necessary training to move toward high proficiency levels.

The IRS agreed to correct reporting inconsistencies and ensure that CSIRC employees and contractors are compliant with specialized security training requirements. The IRS partially agreed to remove system access by removing network access and ensure that employees receive training to achieve high proficiency levels as well as intermediate proficiency levels. The IRS disagreed with capturing the costs of handling and responding to an incident because it is not required by Federal standards. TIGTA agreed that capturing costs is not explicitly required; however, it can help determine if additional funding is needed for the incident response team and can be used to measure the success of the team and effect of changes to capabilities on performance.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

August 28, 2017

MEMORANDUM FOR CHIEF INFORMATION OFFICER

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – The Computer Security Incident Response Center Is Preventing, Detecting, Reporting, and Responding to Incidents, but Improvements Are Needed (Audit # 201620003)

This report presents the results of our review to evaluate the effectiveness of the Internal Revenue Service's (IRS) Computer Security Incident Response Center at preventing, detecting, reporting, and responding to computer security incidents targeting IRS computers and data. This audit is included in our Fiscal Year 2017 Annual Audit Plan and addresses the major management challenge of Security Over Taxpayer Data and Protection of IRS Resources.

Management's complete response to the draft report is included as Appendix VII.

Copies of this report are also being sent to the IRS managers affected by the report recommendations. If you have any questions, please contact me or Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services).

Table of Contents

Appendices

Abbreviations

CSIRC	Computer Security Incident Response Center
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
IRM	Internal Revenue Manual
IRP	Incident Response Plan
IRS	Internal Revenue Service
IT	Information Technology
NIST	National Institute of Standards and Technology
OI	Office of Investigations
PII	Personally Identifiable Information
SOP	Standard Operating Procedures
TCSIRC	Department of the Treasury Computer Security Incident Response Center
TIGTA	Treasury Inspector General for Tax Administration
US-CERT	United States Computer Emergency Readiness Team

Background

The Federal Information Security Modernization Act of 2014 (FISMA)[1] specifically directs Federal agencies to develop and implement procedures for preventing, detecting, reporting, and responding to computer security incidents. The Internal Revenue Service (IRS) implements these requirements through its Computer Security Incident Response Center (CSIRC), which serves as a mechanism for receiving and disseminating computer security incident information and provides a consistent capability to respond to and report cyber-related incidents. The CSIRC possesses capabilities that monitor, detect, and mitigate cyber threats from various sources and includes a technical team that provides deployment, maintenance, and administration of CSIRC security detection, prevention, monitoring, analysis, and reporting devices. This includes information systems used by Operations and Emerging Threat analysts.

The CSIRC's mission is to be proactive in preventing, detecting, and responding to computer security incidents targeting the IRS's enterprise information technology assets, to provide assistance and guidance in incident response, and to provide a centralized approach to incident handling across the IRS enterprise. Its responsibilities include ensuring that the IRS has a team of capable "first responders" organized, trained, and equipped to identify, contain, and eradicate cyber threats targeting IRS computing assets using industry best practice tools, tactics, techniques, and procedures. One of the primary duties of the CSIRC is to perform 24-hour monitoring and provide support to IRS operations, seven days a week, 365 days a year.

CSIRC operations have become more and more important as cybersecurity threats against the Federal Government continue to be reported each year. According to the Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT),[2] Federal agencies reported 77,183 cyberattacks in Fiscal Year (FY) 2015, an increase of approximately 10 percent from FY 2014. We were unable to compare the FY 2015 cyberattacks to the reported incidents for FY 2016[3] because Federal agencies were required to use a different reporting requirement. Because the IRS maintains tax information on all taxpayers, the IRS is an attractive target for hackers. Weaknesses in the CSIRC program could prevent the timely detection, prevention or reporting of unauthorized access and disclosure of taxpayer data.

For FY 2016 (through April 2016), the IRS reported 364 incidents, which included 225 loss or theft of equipment, 71 external or removable media, and eight web attacks. Among these cyber incidents was one in which the IRS announced on February 9, 2016, that it had identified and halted an automated botnet attack on its e-file Personal Identification Number application on

[1] Pub. L. No. 113-283.

[2] See Appendix VI for a glossary of terms.

[3] Office of Management and Budget, *Annual Report to Congress: Federal Information Security Modernization Act* (Mar. 2017). Agencies reported 30,899 incidents to US-CERT in FY 2016 using the revised guidelines.

IRS.gov. The attack was designed to generate e-filing Personal Identification Numbers, which would presumably be used to request fraudulent tax refunds. Using personal data stolen outside the IRS, identity thieves used malware in an attempt to generate e-file Personal Identification Numbers for stolen Social Security Numbers. While the botnet attack did not compromise the IRS system or disclose any personal taxpayer data, this cyberattack, along with the Get Transcript attack and the eight web attacks, highlight the prominence of the IRS as a target. In July 2016, a Department of Homeland Security executive stated that "Cyber adversaries have no lawyers, no rules and plenty of money. All they have to do is execute. We have to protect a way of life."[4]

The Treasury Inspector General for Tax Administration (TIGTA) previously issued two audit reports in 2012 and 2015[5] that contained eight recommendations related to computer security incident handling. IRS management disagreed with one of the eight recommendations and did not take any corrective actions for us to evaluate. For the remaining seven recommendations, TIGTA recommended that the CSIRC:

1) Develop a data warehouse capability to reconcile active servers connected to the IRS network with servers monitored by the Host-Based Intrusion Detection System.

2) Revise and expand the Memorandum of Understanding with the TIGTA Office of Investigations (OI) for the sharing of relevant security incidents with the CSIRC.

3) Collaborate with TIGTA OI to create common identifiers to help the CSIRC and TIGTA OI reconcile their incident tracking systems.

4) Develop a standalone incident response policy or update the policy in the IRS's Internal Revenue Manual (IRM) with current and complete information.

5) Develop an incident response plan.

6) Develop, update, and formalize all critical standard operating procedures (SOP).

7) Ensure that a proposed task order is awarded and includes language that security incident reports contain detailed investigation documentation for all potential or suspected incidents detected and investigated by an IRS contractor's security operations team.

This review was performed at the CSIRC operations within the Information Technology (IT) organization's Cybersecurity organization in Lanham, Maryland, during the period February 2016 through February 2017. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the

[4] Mark Rockwell, *Cyber worker shortage hurting operations*, Federal Computer Weekly, July 27, 2016.
[5] TIGTA, Ref. No. 2012-20-019, *The Computer Security Incident Response Center Is Effectively Performing Most of Its Responsibilities, but Further Improvements Are Needed* (Mar. 2012), and TIGTA, Ref. No. 2015-20-008, *Security Enhancements Are Needed to Better Protect Tax Return Information That Passes Through the Integrated Enterprise Portal–Registered User Portal* (Jan. 2015).

audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Results of Review

The CSIRC has generally followed Federal requirements for handling cybersecurity incidents. Nonetheless, there are areas in which the CSIRC could improve its operations. Specifically, we identified improvements are needed in reporting incidents for a single threat vector to the Department of the Treasury CSIRC (TCSIRC); consistently applying reporting procedures for like incidents by threat vectors; updating the CSIRC Incident Response Plan (IRP); and meeting FISMA training requirements for employees and contractors as well as specialized security training for employees.

Correcting these areas will improve the CSIRC's effectiveness in preventing, detecting, reporting, and responding to cybersecurity incidents targeting IRS computers and data. In addition, providing specialized security training, such as participating in exercises that include current exploits and keeping up with industry trends for its first responders despite the perceptions about the locations of the training, will assist with the CSIRC's effectiveness to combat attacks targeting the IRS.

Planned Corrective Actions for Computer Security Incident Handling Related Weaknesses Were Generally Implemented

For the seven recommendations from the two TIGTA audit reports, we determined whether the previously reported weaknesses and planned corrective actions were fully implemented, validated, and properly closed. We found that five were fully implemented, one was no longer applicable, and one was partially implemented, which is addressed later in this report.

Five corrective actions were fully implemented

- Revise and expand the Memorandum of Understanding with the TIGTA OI to ensure that all reportable and relevant security incidents are shared with the CSIRC. The scope of the Memorandum is limited to include a computer security incident type that is "Loss or Theft of IT Asset" incidents. We conducted a reconciliation of incidents between the TIGTA OI and the CSIRC on Loss of IT equipment for FYs 2015 and 2016 (through April 30, 2016), and all incidents were accounted for between the two systems.

- Collaborate with the TIGTA OI to create common identifiers to help the CSIRC reconcile its incident tracking system with the TIGTA OI's incident system. The two common identifiers are TIGTA Compliant Number and CSIRC Incident identification and are tracked by both the CSIRC and the OI. As reported in the prior bullet, we conducted a reconciliation and accounted for all incidents.

- Develop a standalone incident response policy or update the policy in the IRS's IRM with current and complete information. The IRS updated IRM 10.8.1.4.8, *Incident Response Policy and Procedures*, to contain recommended elements from the National Institute of Standards and Technology (NIST) Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, that included incident response training, handling, monitoring, and reporting.

- Develop, update, and formalize all critical SOPs. We determined that there were no formal SOPs; rather, only ad hoc SOPs. Ad hoc SOPs were created for a specific event, which may or may not be repeatable. The ad hoc SOPs were not formal documents and were often more detailed procedures. The CSIRC formalized the SOPs, which included critical procedures, with the creation of an IRP. We reviewed the critical procedures cited in the previous TIGTA report and concluded that they were incorporated in the IRP.

- Ensure that the proposed task order is awarded and includes language that security incident reports contain detailed investigation documentation for all potential or suspected incidents detected and investigated by the contractor's security operations team. The security reports should also include incidents from the managed services' subcontractor. The new task order contains a specific section on Security and Privacy and Deliverables for the Ongoing Service Phase. The contractor sends e-mails to the CSIRC and they are recorded as incidents in the Archer system.

One corrective action was no longer applicable

- Develop its Cybersecurity Data Warehouse capability to correlate and reconcile active servers connected to the IRS network with servers monitored by the host-based intrusion detection system. The host-based intrusion detection system platform that was in place on server systems has now been retired in part because the vendor no longer supports the software. The IRS determined that the host-based intrusion detection system phase-out could be achieved securely with the enhancement of network intrusion detection system and endpoint protection security policies.

Incident Handling and Reporting Could Be Enhanced

We reviewed 100 incidents, which consisted of a stratified statistical sample of 96 incidents from a population of 364 incidents for FY 2016 (through April 30, 2016) by threat vector categories[6] and all four FY 2015 incidents with a severity level rating of medium or high[7] as recorded in the

[6] We used a 95 percent confidence level, a 5 percent expected error rate, and ±4 percent precision level to determine whether the CSIRC properly and timely responded to and reported incidents. The strata included all threat vectors with a population count.

[7] At the time of our sample selection, there were no incidents rated with a severity level of medium or high for FY 2016 (through April 30, 2016).

Archer system. Our analysis determined that the CSIRC is generally following Federal requirements and guidance and its own internal policies and procedures for handling and reporting cybersecurity incidents, along with incidents involving loss and theft of equipment. However, we identified some instances in which the CSIRC did not always follow the guidance, policies, and procedures.

The CSIRC was generally following Federal requirements and internal guidance

- The CSIRC properly identified and documented the type, nature, and scope of all 100 incidents, such as identifying the systems and applications affected, the source of the incident, and the specific kind of lost equipment.
- For incidents that required referral to the appropriate internal organizations for further review and action, we found:
  - ➢ The CSIRC properly referred to the Privacy Policy and Compliance office's Incident Management and Employee Protection office[8] all 14 incidents involving 49 pieces of equipment that were lost or stolen and potentially contained Personally Identifiable Information (PII) for 856 employees and 48 taxpayers.

    We further determined that 22 (45 percent) of the 49 pieces of equipment reported lost or stolen with potential PII were encrypted to prevent unauthorized access. Three (6 percent) of the 49 pieces of equipment were not encrypted. The three items were a backup tape, a server, and a network switch. For the remaining 24 (49 percent) pieces of equipment, the Archer system showed the encryption status was unknown. The equipment consisted of four laptops, 19 desktops, and one BlackBerry®.

    While the CSIRC is not responsible for encrypting equipment, the IRS does have a policy that addresses encryption for all portable devices and storage controls for digital media. The Incident Management and Employee Protection office properly processed each incident by assessing the incident and taking the necessary actions, such as sending notices and offering credit monitoring services to affected employees and taxpayers, when the individuals could be identified.
  - ➢ The CSIRC properly documented referrals of four incidents to the IRS Labor Relations office for review of possible employee personnel actions. All four incidents involved improper usage of IRS computer systems in which employees transmitted IRS system login credentials to personal external e-mail accounts. These actions violated IRS and Federal Government policies and guidelines. We did not

[8] The office is located in the IRS Office of Privacy, Governmental Liaison, and Disclosure. The Privacy Policy and Compliance office is the "go-to" organization for areas that include privacy-related inquiries, e-mail containing PII, and compliance with FISMA.

follow up to determine whether personnel actions were taken on these employees because it was outside the scope of our review.

All incidents for threat vectors were not reported as required

- Of the 100 incidents, we determined that 64 incidents were confirmed to have compromised the confidentiality, integrity, or availability of a Federal Government information system and were required to be reported to the TCSIRC. The Department of the Treasury Chief Information Officer Memorandum 15-05, Update to Treasury Directive Publication 85-01, *Treasury Information Technology Security Program, Appendix A: Minimum Standard Parameters and Treasury Controls*, requires that bureaus shall report confirmed cybersecurity incidents to the Government Security Operations Center through the TCSIRC within one business day. Suspected incidents and unsuccessful attacks deemed significant by the bureau shall be reported within three business days. The remaining 36 incidents were not required to be reported because they were unsuccessful incidents or the reporting requirement was optional. The 36 incidents involved loss or theft of equipment, web attack, e-mail attack, and external removable media threat vectors. These threat vectors could include such items as air cards, attempted accesses, passive scans, phishing attempts, or thwarted exploits.

  - ➢ The CSIRC properly reported 42 (66 percent) of the 64 incidents that were required to be reported to the TCSIRC. For the 42 incidents that were properly reported, 41 (98 percent) were timely reported within one business day. The remaining incident was reported 119 days after the incident was confirmed.

  - ➢ The remaining 22 incidents (34 percent) were not reported to the TCSIRC as required. Cybersecurity organization management agreed that these 22 should have been reported to the TCSIRC, but had not reported them. On February 15, 2017, after bringing the noncompliance to the IRS's attention, the 22 were reported to the TCSIRC. Based upon projections from our sample, we estimate that 80 of the 364 incidents in the Archer system involving loss or theft of equipment were not reported to the TCSIRC as required.[9]

    As a remedy for the exceptions, Cybersecurity organization management offered, as a component of quality assurance, to formulate processes that identify and mitigate such lapses in processes.

    Management Action: After the completion of fieldwork, Cybersecurity organization management provided us with a description of the new quality assurance process and

[9] One of the 22 incidents was from the four FY 2015 incidents with a severity level rating of medium or high. For projection purposes, we removed the one incident, which resulted in 21 incidents. The point estimate projection for the 21 is based on a 95 percent confidence interval. We are 95 percent confident that the point estimate is between 59 and 113 potential incidents that were not reported to the TCSIRC.

the date it became effective. Regarding the projections from our sample, Cybersecurity organization management stated they exercised diligence and reviewed all remaining cyber incidents for the specific time frame and ensured that all events were properly reported according to established policy and procedures. Because this information came to us after the end of our fieldwork, we did not have sufficient time to review and verify the quality assurance process to determine whether it will remedy the identified weaknesses or whether all remaining cyber incidents were reviewed and properly reported.

Documentation of actions taken regarding some incidents was insufficient

- Of the 100 incidents, we determined that 54 incidents involved noncompliance with the IRM and/or Law Enforcement Manual; loss or theft of information technology equipment; malicious code (successful and unsuccessful incidents); and web attacks. These incidents occurred through threat vectors such as e-mail attacks, external/removable media, improper usage, the loss or theft of equipment, and web attacks. The CSIRC properly documented the actions to halt the spread of or limit the damage caused by the incident, or documented the effectiveness of its containment actions in 46 (85 percent) of the 54 incidents. The NIST Special Publication 800-61, *Computer Security Incident Handling Guide*, recommends an incident response team that suspects an incident has occurred should immediately start recording all facts regarding the incident. Documenting system events, conversations, and observed changes in files can lead to a more efficient, more systematic, and less error-prone handling of the problem. Every step taken from the time the incident was detected to its final resolution should be documented and timestamped. Every document regarding the incident should be dated and signed by the incident handler. Information of this nature can also be used as evidence in a court of law if legal prosecution is pursued.

  For the remaining eight incidents that were all loss or theft of information technology equipment, actions were missing or incomplete. Cybersecurity organization management agreed with the exceptions and offered to correct the incomplete documentation. The eight exception incidents involved four BlackBerrys and four cell phones. Two BlackBerrys were reported to contain PII for 356 individuals. The remaining two BlackBerrys and four cell phones were reported to contain no PII or its presence was unknown. While the BlackBerrys were reported to the TCSIRC, the four cell phones were among those not reported to the TCSIRC. Based upon projections from our sample, we estimate that 30 of the 364 incidents in the Archer system were missing or had incomplete documentation regarding the actions to halt the spread of or limit the damage caused by the incident, or the effectiveness of its containment actions.[10]

Incident costs were not captured

- For all 100 incidents, the CSIRC did not capture the costs of handling and responding to the incidents. Cybersecurity organization personnel responded that, although the NIST is promulgating guidance to the Federal Government community, no mandate exists to track associated dollar cost. They also cited that the Impact and Severity Assessment serves the purpose to identify the varied impacts of the incident. This Assessment factors in functional impact, information impact, and recoverability. We reviewed the referenced Assessment and disagree that it addresses the cost capturing weakness we identified.

  The NIST Special Publication 800-61, *Computer Security Incident Handling Guide*, recommends certain post-incident data can be used to improve the handling of future incidents. Data such as the total hours and cost of involvement may be used to justify additional funding of the incident response team. After handling an incident, an agency should issue a report that details the cost of the incident, among other information.

  In addition, the Presidential Policy Directive, *United States Cyber Incident Coordination*, dated July 26, 2016, requires that when a Federal agency is the target of a cyber incident, it is to manage the effects of the incident on the agency's operations, customers, and workforce. The means of managing the effects include addressing financial impacts.

  While there is no requirement to track and monitor cost data, such data can help determine if additional funding is needed for the incident response team. It can also be used to measure the success of the incident response team and the effect of changes to incident response capabilities on performance, *i.e.*, improvements in efficiency and reductions in costs. The Government Accountability Office selected and reviewed six Federal agencies to determine adherence to Federal guidance. In its April 2014 Cyber Incident Response review, the Government Accountability Office reported the same issue for the six Federal agencies that it evaluated (the evaluation did not include the Department of the Treasury). Those agencies did not generally capture cost information.[11]

[10] The point estimate projection is based on a 95 percent confidence interval. We are 95 percent confident that the point estimate is between 16 and 53 potential incidents that were missing or had incomplete documentation of actions that were taken while working the incidents.

[11] Government Accountability Office, GAO-14-354, *Information Security: Agencies Need to Improve Cyber Incident Response Practices* (April 30, 2014).

Reporting procedures were inconsistently applied

We identified following two areas of reporting inconsistencies during our review of the 100 incidents.

- Twelve (12 percent) of the sampled incidents involved the loss or theft of a cell phone or BlackBerry.
    - In two incidents, the employees initially reported the cell phones did not contain any PII. However, after the Information System Security Officer questioned whether the cell phones contained the names and numbers of IRS employees and other Federal agency employees, the Information System Security Officer requested that the CSIRC update the reports. In addition, the CSIRC referred one of the two incidents to the Incident Management and Employee Protection office as possibly containing PII for further review. Both incidents were reported to the TCSIRC, as required.
    - In eight incidents in which the employees reported the cell phones or BlackBerrys did not contain any PII, an additional probe for PII was not performed to decide whether the reports should be updated and subsequently referred as containing possible PII such as names and phone numbers. Six of the eight incidents were part of the 22 incidents we previously reported that were not reported, as required, to the TCSIRC.

      After completion of fieldwork, Cybersecurity organization management stated the eight incidents were updated within the Archer system to reflect that each of the assets did indeed contain an unknown quantity of PII – primarily, names and telephone numbers. Additionally, the Incident Management and Employee Protection office was provided a communication to reflect that the incidents had been updated within the Archer system to reflect the PII status. We verified the eight had been updated within the Archer system and that the Incident Management and Employee Protection office were appropriately updated.
    - In two incidents, the employees indicated PII was included or it was unknown whether PII was present on the BlackBerrys. Both incidents were reported to the TCSIRC, as required.

      Based upon the projections from our sample, we estimate that 38 incidents in the Archer system may have been referred to the Incident Management and Employee Protection office with an incorrect status of not containing PII on a BlackBerry or cell phone because there was no additional probing for PII.[12] Consequently, the CSIRC was not afforded the opportunity to update the lost or stolen incident reports. We did

[12] The point estimate projection is based on a 95 percent confidence interval. We are 95 percent confident that the point estimate is between 21 and 62 potential incidents that may not have been referred to the Incident Management and Employee Protection office as possibly containing PII on a BlackBerry or cell phone.

not make any projections on the incidents that were not reported to the TCSIRC because they were included in an earlier projection.

We suggested to Cybersecurity organization management that the CSIRC should ask probing questions when smart phones such as cell phones and BlackBerrys are reported lost or stolen to ensure proper reporting. Cybersecurity organization management responded that the incident reporting form has probing questions, such as names, Social Security Numbers, and date of birth, that the CSIRC uses. The CSIRC is responsible for input of all incidents and reportable content to the Archer system. While the incident reporting form includes examples of PII and Cybersecurity organization management stated they are used, our audit results demonstrated a weakness in the CSIRC's use of the form during the input process. We believe a refresher training is needed in determining PII when lost or stolen cell phones or BlackBerrys are reported. It is common knowledge that cell phones and BlackBerrys can store PII when they have been used, whether to send an e-mail or to store frequently used numbers.

After completion of fieldwork, Cybersecurity organization management provided documentation of actions they have taken and assurances of ongoing actions regarding PII and other conditions we identified with the sampled incidents. They implemented a combination of "brown-bag" sessions to provide greater familiarity and insight into CSIRC processes or technologies and also a daily series of incident-driven scenarios to be executed during daily stand-up calls. In addition, we verified the notification actions for lost or stolen cell phones and PII from the IT organization's User and Network Services office. Therefore, we did not make a recommendation for this issue.

- Three of the four incidents involving improper usage of IRS computer systems reported to Labor Relations were also reported, as required, to the TCSIRC. However, the remaining incident was not. We did not make a projection on the incident that was not reported to the TCSIRC because it was included in an earlier projection.

Management Action: As a remedy for the inconsistency exceptions, CSIRC management stated that, as a component of quality assurance, they will formulate a process that identifies and mitigates such lapses. TIGTA received the effective date and information on the new process after the completion of fieldwork. As such, we did not have sufficient time to verify the effective date and review the process to determine whether it will remedy the identified weaknesses.

Recommendations

The Chief Information Officer should ensure that:

Recommendation 1: The CSIRC corrects the reporting inconsistency by reporting the remaining cell phone that contained PII to the Incident Management and Employee Protection office, and correct the missing or incomplete documentation indicating the actions to halt the spread of, limit the damage caused by the incident, and, when applicable, document the effectiveness of the containment actions for the eight incidents.

> ***Management's Response:*** The IRS agreed with this recommendation. The CSIRC has ensured that each of the remaining incidents involving lost/stolen cell phones are properly reflected as containing PII within the CSIRC incident tracking system, along with reporting to the TCSIRC and Office of Privacy, Governmental Liaison, and Disclosure. Supporting TCSIRC tickets numbers have been provided to TIGTA, as evidence of this completion.

Recommendation 2: The costs of handling and responding to an incident are captured for the purposes outlined in the NIST Special Publication 800-61, *Computer Security Incident Handling Guide.*

> ***Management's Response:*** The IRS disagreed with this recommendation. While NIST Special Publication 800-61 notes associated cost as a data element for consideration, this is promulgating guidance and no requirement to track monetary costs currently exists. CSIRC incident tracking aligns with Department of the Treasury and US-CERT reporting requirements and associated data reporting artifacts. Specifically, the Impact and Severity Assessment (factoring in functional impact, information impact, and recoverability) serves this very purpose - to identify functional and information impact, along with level of effort for remediation or recovery. Additionally, the associated Impact and Severity Assessment serves as a determining factor for major or significant incident categorization.

> ***Office of Audit Comment:*** As reported, we reviewed the Impact and Severity Assessment to which the IRS referenced in its response and the assessment does not capture the costs for handling and responding to incidents. While we agree that capturing the costs is not explicitly required, we believe that capturing cost data can help determine if additional funding is needed for the incident response team. It can also be used to measure the success of the incident response team and the effect of changes to incident response capabilities on performance, *i.e.*, improvements in efficiency and reductions in costs.

Employees and Contractors Did Not Always Meet Training Guidelines, and Skill Assessments Demonstrate a Need for More Training

CSIRC staff did not always meet IRS training requirements

The IRS requires two different types of security training for its employees and contractors: specialized role-based security training and general security awareness training.

IRM 10.8.1.4.2.2, *Role-Based Security Training*, states that role-based/specialized security training shall be provided to personnel assigned security roles and responsibilities, which include security specialist. In the CSIRC, employees and contractors are assigned technology security specialist roles and serve as first responders to identify, contain, and eradicate cyber threats targeting IRS computing assets using industry best practice tools, tactics, techniques, and procedures. Personnel performing technical security roles requiring specialized training shall receive a minimum of eight hours of specialized training annually. The IRS defines annual as the FISMA yearly cycle from July 1st to June 30th of the following year. In addition, IRM 10.8.2.2.1.10.1(2)d, *Contracting Officers Representatives*, requires that system owners revoke access privileges in a timely manner when a contractor fails to comply with stated policies or procedures.

Policy and Procedures Memorandum No. 39.1(H), *IRS Specialized Information Technology Security Training (Role-Based)*, states that all contractor employees who have a significant information technology security role shall complete and report training hours within each FISMA cycle. It further provides that the contractor shall submit confirmation of annually completed specialized information technology security training (role-based) using the Government system identified by selected IRS programs for each employee identified, with a copy to the contracting officer and contracting officer representative, upon completion of the training.

NIST Special Publication 800-100, *Information Security Handbook: A Guide for Managers*, defines “awareness” as tools that are used to promote information security and inform users of threats and vulnerabilities that affect their agency and “personal” work environment by communicating information security policies and procedures that need to be followed. In that regard, awareness training provides the foundation for any sanctions and disciplinary actions imposed for noncompliance. Awareness training is used to explain the rules of behavior for using an agency’s information systems and information, and establishes a level of expectation on the acceptable use of the information and information systems. However, the same guidelines explain that specialized training seeks to teach skills that allow a person to perform a specific function. Information security training strives to produce relevant and needed security knowledge and skills within the workforce. Security training supports competency development and helps personnel understand and learn how to perform their security role.

In addition, IRM 10.8.1.4.2.3, *Security Training Records*, states that the IRS shall document and monitor individual information system security training activities including specific information system security training. In addition, the IRS shall retain individual training records for individuals and information systems for a period of five years.

We reviewed the IRS's Enterprise Learning Management System training records to determine whether CSIRC employees met the required specialized security training for the FISMA yearly cycle for two years. In addition, we requested documentation of the specialized security training from those responsible for the contractors for the same periods. For the FISMA 2015 and 2016 yearly cycles, we reviewed all selected CSIRC employees required to complete specialized security training and the courses completed, which included the course objectives. We found that 10 employees in the 2015 yearly cycle and seven employees in the 2016 yearly cycle attained the required eight hours of training that the IRS deemed as specialized. However, after closer examination of the courses completed, we disagreed with the designation and determined that some of the courses were more awareness security training than specialized security training. As a result, for the FISMA 2015 yearly cycle, four of the 10 CSIRC employees met the specialized training requirement and the remaining six did not. For the FISMA 2016 yearly cycle, five of the seven employees did not meet the specialized security training requirements.

We presented our exceptions and the list of 34 courses which we believed were awareness training rather than specialized security training to Cybersecurity organization management. Cybersecurity organization management agreed that seven courses were awareness training. After removing credit for the seven awareness training courses from the employee records, for the FISMA 2015 and 2016 yearly cycles, three and five CSIRC employees, respectively, did not complete the required number of training hours. In addition to the removal, we maintain our concern that the remaining 27 courses may provide awareness training instead of specialized security training.

For the FISMA 2015 yearly cycle, there were no training records available for review to support that the 11 CSIRC contractors met the same requirement. The contracting officer's representative did not have any documentation, such as training certificates, to support that specialized training was provided to the contractors. Cybersecurity organization personnel believed that because the FISMA 2015 yearly cycle training requirement pre-dated the internal guidance to complete and report the specialized training, there was no requirement to forward the documentation to the contracting officer's representative or to maintain it. We disagreed and provided evidence that the FISMA training requirement had been in effect since 2002.

For the FISMA 2016 yearly cycle, 14 (93 percent) of 15 contractors did not meet the specialized security training requirements. The contracting officer's representative provided documentation, but the training was completed after the FISMA 2016 yearly cycle and well into the FISMA 2017 yearly cycle. Also, the 2017 cycle documentation did not provide the number of hours trained to determine whether they met the required number of hours; only the course titles were included. Despite not meeting specialized security training requirements in both FISMA yearly cycles, contractors continued to have system accesses, instead of being removed as required. This occurred because Cybersecurity organization management did not agree that the Policy and Procedures Memorandum required the contractors' access to be removed. We provided the IRM that states system owners are to revoke access privileges when contractors are noncompliant with policies and procedures.

Skills assessment shows a need for training; however, there are challenges associated with providing the training

To its credit, the IRS conducted an assessment of the information technology skills and identified proficiency gaps of its IT organization employees, including CSIRC employees. The skills gap is determined by assessing the employee's current skill levels when compared to the Skills Framework for the Information Age Standards used in private industries. The employees self-assessed their skill levels from 1 to 5[13] for 305 skill areas, and the results were then validated by their manager. In FY 2016, only five of seven[14] senior CSIRC employees completed the assessment. We asked the CSIRC manager to identify the most relevant skills related to the work conducted by the CSIRC, and the manager responded with the top 48 skills. We analyzed the five senior CSIRC employees' proficiency levels for these 48 skill areas to gauge the group's skills proficiency as a whole and found the following:[15]

- 3 skill areas in which no employees were at a proficiency level of 4 or 5. These areas were 1) exploit research development, 2) IPv6 protocol, and 3) SQL injection.
- 9 skill areas in which one employee was at a proficiency level of 4 or 5. These areas were 1) advising information technology experts on security threats to web services, development, or operations; 2) conducting reviews to detect malicious code; 3) Department of Homeland Security guidelines and standards; 4) IRM 10.8 on IT Security; 5) identifying and mitigating risks and vulnerabilities for Linux; 6) identifying and mitigating risks and vulnerabilities for UNIX; 7) social engineering; 8) telecommunications for cybersecurity; and 9) Treasury guidelines and standards.
- 29 skill areas in which two employees were at a proficiency level of 4 or 5.
- 7 skill areas in which three or more employees were at a proficiency level of 4 or 5.

[13] We defined level 1 as not having this skill; level 2 as possessing basic skills, *i.e.*, handle simple tasks; level 3 as possessing intermediate skills, *i.e.*, handle many types of tasks independently; level 4 as possessing advanced skills, *i.e.*, handle nearly all tasks independently; and level 5 as possessing expert skills, *i.e.*, handle all tasks independently and can serve as a coach for others.

[14] The skills assessment was conducted in October 2015 when eight employees were assigned to the CSIRC. One was a manager, who was excluded from completing the assessment. Two additional CSIRC employees started in December 2015 after the assessment had been completed.

[15] Appendix IV contains a list of the top 48 relevant skills for CSIRC employees used in our analysis.

We believe this analysis shows a need for more specialized security training to address deficient skill areas of CSIRC employees.

Challenges associated with obtaining specialized security training

We interviewed Cybersecurity organization and CSIRC personnel regarding training and the challenges associated with obtaining specialized security training. They cited a lack of funding as a main obstacle to training. We requested the training dollars budgeted for the CSIRC and the dollars spent for the employees; however, the budget dollars and the number of slots for employee expenses are maintained for all of the Cybersecurity organization and not for the CSIRC only. Therefore, we were unable to determine the actual training dollars budgeted and expended for CSIRC employees.

Another challenge CSIRC employees cited was the training locations and the approval to attend them. In a survey questionnaire we provided CSIRC employees, the majority responded that better and more training opportunities were needed. They have found private sector specialized training much more helpful and informative because they provide proven defense techniques, coupled with contemporary attack trends, observations, and reports, as well as information on cutting edge attacks and defense methodologies that are missing from courses on the Enterprise Learning Management System. One CSIRC employee noted the reason is that these types of courses are usually held at sites considered to be “luxury” locations.

We met with Cybersecurity organization executives and they stated that they have varied training opportunities, such as those conducted by the Department of Homeland Security and the Treasury Departmental Office. However, they agreed training is an issue. We are concerned with the overall skills of the responders to perform their duties and effectively respond to cybersecurity incidents and other security activities affecting the IRS. Travel cost is a major consideration when selecting any specialized security training class. As such, local training is usually preferable. However, the high cost of these training classes as well as the need to travel may be justified in order to maintain or increase the skill proficiency of the CSIRC staff, particularly if these types of classes are the best or only ones offered throughout the country.

Additionally, we are concerned that insufficient training could lead to employee frustration, which could lead to employees leaving the IRS. CSIRC employees stated in their responses to our questionnaire that they have been asked and have considered leaving. We reviewed the Cybersecurity organization’s Comparison Report in the 2016 Federal Employee Viewpoint Survey results and found that, while 60 percent of the 191 survey respondents agreed that their workforce has the job-relevant knowledge and skills necessary to accomplish organizational goals, 40 percent were either neutral or disagreed. In another question, approximately 72 percent of the 196 survey respondents were either neutral or dissatisfied with the training they received for their present job, and approximately 51 percent were either neutral or did not agree that the skill level in their work unit had improved in the past year.

A study conducted by McAfee,[16] the self-proclaimed world's largest dedicated security company, presented feedback on cybersecurity skills from 775 information technology decision makers involved in their organizations with at least 500 employees in both the public and private sectors from eight countries, including the United States. One of their key findings was that a shortage of cybersecurity skills makes their organizations more desirable hacking targets.

Recommendations

The Chief Information Officer should ensure that:

Recommendation 3: CSIRC employees and contractors are FISMA compliant with the specialized security training requirement during the FISMA annual cycle. In addition, contractor training documentation should include the number of hours trained, which would assist in determining whether the required number of hours had been completed.

> ***Management's Response:*** The IRS agreed with this recommendation. On July 11, 2016, the IRS implemented new technology, policy, and process changes to provide, gather, track, and monitor security training execution for contractors and employees. For the 2017 FISMA reporting period, the IT organization, including the CSIRC, achieved 100 percent compliance for both contractors and employees. The FISMA Archer system and the Enterprise Learning Management System are leveraged to provide, collect, track, and report training compliance including the number of training hours assigned and completed. In addition to automated tools, the IRS maintains numerous subject matter experts to assist in the review of assignment and completion documents.
>
> ***Office of Audit Comment:*** Our review of the FISMA 2017 yearly cycle documentation showed that the number of training hours for the contractors was not available to determine whether the contractors met the required number of hours to be FISMA compliant.

Recommendation 4: System owners remove CSIRC contractors' access privileges to IRS systems when they are noncompliant with FISMA training requirements.

> ***Management's Response:*** The IRS partially agreed with this recommendation. The IRS implemented systemic de-provisioning at the network access point to ensure that all access would be eliminated instead of relying on individual system owners to remove access privileges as recommended by TIGTA. On March 6, 2017, prior to the issuance of this draft report, the IRS had already fully implemented new technology, policy, and process changes to de-provision FISMA noncompliant contractors from accessing the IRS network. This de-provisioning process is executed weekly for Information Systems

[16] McAfee, *Hacking the Skills Shortage: A Study of the International Shortage in Cybersecurity Skills,* p. 4 (Jul. 2016).

Security training and for annual Specialized Information Technology Security training prior to the June 30, 2017, FISMA year-end date.

> ***Office of Audit Comment:*** We concur with the IRS's alternative corrective action to this recommendation. While we did not evaluate the effectiveness of this corrective action, we believe it will remove system access for noncompliant contractors.

Recommendation 5: CSIRC employees receive the necessary specialized security training to reduce the skills gap and become more proficient toward levels 4 and 5. In addition, consider specialized security training for all first responders that promotes current, real life cyberattack situations and technology exercises, which includes those locations where the training cannot be obtained elsewhere.

> ***Management's Response:*** The IRS partially agreed with the recommendation. The IRS will continue to develop its employees to the appropriate proficiency level for their duties and grade level as specified in their position descriptions. However, the IRS does not agree that an intermediate proficiency level (level 3) is a deficiency. The Cybersecurity organization considers virtual and in-person training at on-site and off-site locations for those critical skillsets deemed essential for maintaining organizational performance. However, these locations must comply with IRS guidelines that have been implemented to maintain the integrity of the IRS and public trust.

> ***Office of Audit Comment:*** The IRS agreed to develop its CSIRC employees, but not necessarily towards a proficiency level of 4 and 5, which we maintain should occur to assist the IRS with meeting its defensive strategy against increasing cyber threats.

The Incident Response Plan Was Developed, but It Needs Updating to Comply With Federal Guidelines

We stated earlier in this report that the corrective actions for one of seven recommendations from a TIGTA report in 2012 was partially implemented. The recommendation was for the CSIRC to develop a standalone IRP that includes the elements recommended by the NIST, specifically the NIST Special Publication 800-61 Revision 2, *Computer Security Incident Handling Guide*. We reviewed the Joint Audit Management Enterprise System for the IRS's response, documentation, and status of the planned corrective action. The corrective action for the recommendation was closed December 2012, indicating that the corrective action was completed.

As reported earlier, we determined that IRS management updated the IRM with recommended elements from the NIST Special Publication 800-53 that included incident response training, handling, monitoring, and reporting. We compared the IRM and NIST guidance to the IRP and reviewed Federal regulations for additional guidance. Generally, CSIRC IRP guidelines and procedures addressed most key elements required by Federal regulations and NIST recommendations that were included in the IRM, but the plan needs updating. Figure 1 presents the results of our analysis of the CSIRC IRP that shows the plan did not include or partially addressed nine (28 percent) of 32 NIST recommended elements applicable to the IRP in the areas of policy, plan, procedure, and sharing (interactions) with outside parties.[17]

Figure 1: Assessment of the CSIRC IRP Containing the Number of NIST Recommended Elements

NIST Element Categories	Number of Elements Recommended	Number of Elements Not Included in the IRP	Number of Elements Partially Addressed in the IRP	Number of Elements Included in the IRP	Number of Elements Not Applicable to the IRP
Policy	8	1	2	5	0
Plan	10	3	2	5	0
Procedure	9	0	0	9	0
Sharing (Interactions) With Outside Parties	10	0	1	4	5
Totals	**37**	**4**	**5**	**23**	**5**

Source: TIGTA's analysis of the CSIRC IRP.

Specifically, the CSIRC IRP did not include or only partially addressed the following NIST elements in the plan.

<u>Policy elements</u>

- **Statement of management commitment** (Not included in the IRP).
- **Establish performance measures** (Partially addressed in the IRP). The CSIRC IRP contains examples of elements to be assessed and/or measured for determining the effectiveness of the overall incident response process, which feeds information back into the preparation phase. However, the plan neither describes how these elements can or will be used to measure the effectiveness of the program. The IRP includes information on evaluating the timeliness of the response, but does not specify the frequency of measuring the timeliness of the response, *i.e.*, after every incident, once a week for all incidents, or after a predetermined number of incidents. Also, there are other precision measurements that the CSIRC could use to evaluate the incident response process. For example, the IRP could include measuring the total time per incident such as total

[17] There are 37 elements that the NIST recommended for the IRPs; however, five elements are not applicable to the IRS. These elements refer to policy and procedures when interacting with the media. The IRP provides an overall statement that all media contacts and questions are handled by the IRS Media Relations office. The 37 elements are listed in Appendix V.

number of labor hours spent working an incident, and notifying the appropriate internal and external offices such as the Privacy Policy and Compliance office's Incident Management and Employee Protection office, the TCSIRC, and the TIGTA OI. An additional measurement for the IRP could include measuring whether PII was correctly reflected when lost or stolen equipment was reported in the Archer system.

- **Define organizational structure, roles, responsibilities, and levels of authority, specifically the requirement for reporting certain types of incidents** (Partially addressed in the IRP). The CSIRC IRP contains reporting requirements, but it was not updated to reflect current requirements of reporting confirmed incidents to the TCSIRC within one business day and reporting suspected incidents and unsuccessful attacks deemed significant by the IRS within three business days.

Plan elements

- **Strategies and goals** (Not included in the IRP).
- **Senior management approval** (Not included in the IRP).
- **Information Technology roadmap for maturing the incident response capability** (Not included in the IRP). With information technology constantly evolving and the increase in hacking and malicious code attacks, it is essential the CSIRC establish a roadmap to keep up with the changing environment. The roadmap should include items such as software and hardware upgrades (including timelines, costs, *etc*.) to maintain the ability to respond to all types of system intrusions, staffing increases or changes, training goals for first responders, and timelines for updating the IRP.
- **Metrics for measuring the incident response capability and its effectiveness** (Partially addressed in the IRP). Reports, such as the Cyber Daily and Cyber Quarterly Reports, were identified in the IRP, but there is no statement that provides how these reports are used to evaluate the effectiveness of the incident response program.
- **How the program fits into the overall organization** (Partially addressed in the IRP). Reference is made to the roles and responsibility section of the plan, but it does not provide context on how the CSIRC fits into the organizational structure of the IRS.

Sharing (Interactions) with outside parties element

- **Document all contacts and communications with outside parties for liability and evidentiary purposes** (Partially addressed in the IRP). The plan does provide for analysts to document analyses performed on an incident; however, it does not include guidance to document all contacts and communications.

Cybersecurity organization management stated that the NIST serves as promulgating guidance and does not specifically mandate any of the elements we identified. They believed that the CSIRC IRP contained the elements deemed essential to ensuring an efficient and effective incident response capability, along with proper alignment with Federal regulations mandated by the Office of Management and Budget, US-CERT, and the Department of the Treasury policy. We reminded Cybersecurity organization management that they agreed to update the IRM with the NIST guidelines. Therefore, the IRM mandates that the IRP reflect the elements it adopted from the NIST and the Department of the Treasury.

Establishing and maintaining a current, accurate, and complete incident response policy will provide the program with clear procedures. According to the NIST, once an organization develops a plan and gains management approval, the organization should implement the plan and review it at least annually to ensure that the organization is following the roadmap for maturing the capability and fulfilling its goals for incident response.

Other concerns with the IRP

The CSIRC IRP is not updated with current incident reporting, IRS organizational, and technology information.

- The IRP is organized by incident and event categories, rather than by threat vector categories. The 2016 FISMA Annual Report to Congress states that the US-CERT's revised Incident Notification Guidelines require agencies to use an incident reporting methodology that classified incidents by the method of attack vectors, which is synonymous with threat vectors. While the CSIRC has been reporting to the TCSIRC, the IRP has not been updated to reflect this new reporting requirement and the time frames associated with them. CSIRC management indicated the event categories are used internally. We considered the internal use and concluded that the IRP should be organized by the new threat vectors and include the associated incident and event categories, because both are used.
- There are references to an IRS organization, End User Equipment and Services, that no longer exists. On April 22, 2012, this organization was merged with the Enterprise Network organization to form the new User and Network Services organization.
- The IRP cites computer hard drive protection with Guardian Edge technology, which was replaced with Symantec Endpoint Encryption technology in July 2012.
- There are IRM citations in the plan that are no longer valid.

The IRS has specific guidance over the closure of weaknesses reported for its internal control program. The IRM 1.4.30, *Monitoring Internal Control Planned Corrective Actions*, requires that recommendations are appropriate and implemented, corrective actions are taken in a timely fashion through independent verification, and that validations occur. In addition, the Government Accountability Office guidance provides that management should complete and document corrective actions to remediate internal control deficiencies on a timely basis. The corrective action is completed only after action has been taken that 1) corrects identified deficiencies, 2) produces improvements, or 3) demonstrates that the findings and recommendations do not warrant management action.

Management Actions: On May 23, 2017, after completion of fieldwork, Cybersecurity organization management provided evidence of the updates to the IRP demonstrating their compliance with Federal guidelines. We reviewed the revised IRP and concur that the weaknesses we identified during the audit have been corrected. Therefore, we did not make a recommendation for this issue.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to evaluate the effectiveness of the CSIRC at preventing, detecting, reporting, and responding to computer security incidents targeting IRS computers and data. To accomplish our objective, we:

I. Determined whether previous reported weaknesses and planned corrective actions from the 2012 and 2015[1] TIGTA reports[2] were fully implemented, validated, and properly closed.

II. Determined whether the CSIRC IRP established policies and procedures that conform to the NIST, Office of Management and Budget, Department of the Treasury, Executive Order, and IRS requirements on computer security incident handling.

III. Determined whether the CSIRC has a team of capable "first responders" that conforms to the policies and procedures for preventing computer security incidents.

   A. Determined whether the CSIRC incident response team received the necessary and appropriate training. We reviewed all selected CSIRC employees required to complete specialized security training and the courses completed, which were 10 employees in the FISMA 2015 yearly cycle and seven employees in the FISMA 2016 yearly cycle.

   B. Interviewed Cybersecurity organization and CSIRC personnel, and used a questionnaire to determine whether CSIRC personnel had the necessary tools and resources to be effective "first responders" to address computer security incidents.

IV. Determined whether the CSIRC is effectively detecting computer security incidents.

V. Determined whether the CSIRC is effectively responding to and reporting computer security incidents.

   A. Selected a stratified statistical sample of 96 incidents from 364 FY 2016 (through April 30, 2016) incidents recorded on the Archer system[3] and all four FY 2015

[1] For this review, the audit team followed up on only the recommendations that related to computer security incident handling with which the IRS agreed with the recommendation.

[2] TIGTA, Ref. No. 2012-20-019, *The Computer Security Incident Response Center Is Effectively Performing Most of Its Responsibilities, but Further Improvements Are Needed* (Mar. 2012), and TIGTA, Ref. No. 2015-20-008, *Security Enhancements Are Needed to Better Protect Tax Return Information That Passes Through the Integrated Enterprise Portal–Registered User Portal* (Jan. 2015).

[3] See Appendix VI for a glossary of terms.

incidents with an incident severity level of medium and high to determine whether the CSIRC properly and timely responded to and reported the incidents. We used a stratified statistical sample to ensure sufficient coverage in threat vectors, including incidents involving loss or stolen PII and to project the review results.

We used a 95 percent confidence level, a 5 percent expected error rate, and a ± 4 percent precision level to determine whether the CSIRC properly and timely responded to and reported incidents. The strata included all threat vectors with a population count. In addition, we consulted with TIGTA's statistician to ensure that the stratified statistical sample size and projections are accurate and verified the reliability of the data during each incident reviewed.

1. Reviewed the incidents to determine whether the CSIRC timely and properly responded to and reported the incident to the TCSIRC. Also, we captured and categorized by source each incident to determine whether the CSIRC is effectively detecting computer security incidents with tools available to it.
2. Determined whether the incident was referred to and properly handled by the Office of Privacy, Governmental Liaison, and Disclosure, and the Privacy Policy and Compliance office's Incident Management and Employee Protection office, if applicable.

Internal controls methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our audit objective: the IRM for information technology security, policy, and guidance; the CSIRC IRP; the US-CERT guidelines on Federal incident notifications; the TCSIRC reporting procedures; the NIST guidelines for cybersecurity definitions, policy, and procedures; and the Office of Management and Budget memoranda. We evaluated these controls by interviewing Department of the Treasury; IRS Cybersecurity organization; IRS Office of Privacy, Governmental Liaison, and Disclosure, Incident Management and Employee Protection office; and TIGTA OI personnel, and by reviewing cyber incidents captured on the CSIRC's Archer system.

Appendix II

Major Contributors to This Report

Danny Verneuille, Acting Assistant Inspector General for Audit (Security and Information Technology Services)
Kent Sagara, Director
Deborah Smallwood, Audit Manager
Louis Lee, Lead Auditor
Cindy Harris, Senior Auditor
Larry Reimer, Senior Auditor
Michael Segall, Senior Auditor
Thomas Martin, Information Technology Specialist

Appendix III

Report Distribution List

Commissioner
Office of the Commissioner – Attn: Chief of Staff
Deputy Commissioner for Operations Support
Deputy Chief Information Officer for Operations
Associate Chief Information Officer, Cybersecurity
Associate Chief Information Officer, User and Network Services
Director, Privacy, Governmental Liaison, and Disclosure
Director, Procurement
Director, Office of Audit Coordination

Appendix IV

The 48 Most Relevant Skills Related to Work Conducted by the Computer Security Incident Response Center

Count	Most Relevant Skills by Name
1	Advising information technology experts on security threats to web services development/operations.
2	Analyzing risk/recommending mitigation procedures.
3	Analyzing/exploiting data from compromised systems.
4	ArcSight[1] incident detection.
5	ArcSight reporting.
6	Availability/authentication/confidentiality/integrity.
7	Conducting audit trails.
8	Conducting Intrusion Detection System configuration/implementation/deployment.
9	Conducting reviews to detect malicious code.
10	Continuous monitoring for cybersecurity.
11	Describing risk assessment methodology/identifying risk/business impact/making recommendations to executives.
12	Determining effectiveness to infect systems.
13	Developing security policies/procedures.
14	Department of Homeland Security guidelines/standards.
15	Ensuring security-related components are configured accordingly.
16	Exploit research/development.
17	FISMA.

[1] See Appendix VI for a glossary of terms.

Count	Most Relevant Skills by Name
18	Identifying security issues/considerations for applicability/risk.
19	Identifying tools/techniques/procedures used to gain access.
20	Identifying/mitigating risks/vulnerabilities for Linux.
21	Identifying/mitigating risks/vulnerabilities for UNIX.
22	Identifying/mitigating risks/vulnerabilities for Windows.
23	Interpreting/documenting information technology security controls.
24	IPS - Intrusion Protection System.
25	Internet Protocol version 4 (IPv4) protocols.
26	Internet Protocol version 6 (IPv6) protocols.
27	IRM 10.8 - Information Technology Security.
28	Information technology security.
29	Managing adherence to security policies/standards/guidelines for workgroups.
30	McAfee/Symantec.
31	Mitigating computer incidents.
32	NIST 800-53.
33	Performing vulnerability analysis/responding to software/hardware vulnerabilities.
34	Preparing security incident response/handling.
35	Prioritizing computer incidents.
36	Providing customers understanding/explanation of IRM security policies.
37	Reading/analyzing/interpreting packet and network captures using Tcpdump.
38	Reading/analyzing/interpreting packet and network captures using Wireshark.
39	Recommending security corrections to mitigate weaknesses.
40	Reporting computer incidents to management.
41	Social engineering.
42	Sourcefire.
43	Structured Query Language injection.
44	Transmission Control Protocol/Internet Protocol.

Count	Most Relevant Skills by Name
45	Telecommunications for cybersecurity.
46	Treasury guidelines/standards.
47	Troubleshooting/mitigating virus/malware to isolate it.
48	Vulnerability analysis techniques.

Appendix V

The National Institute of Standards and Technology's[1] 37 Recommended Elements Related to Incident Responses by Category

8 Elements for the Policy Category:
Statement of management commitment.
Purpose and objectives of the policy.
Scope of the policy (to whom and what it applies and under what circumstances).
Definition of computer security incidents and related terms.
Define organizational structure, roles, responsibilities, and levels of authority.
Prioritization or severity ratings of incidents.
Establish performance measures.
Reporting and contact forms.
10 Elements for the Plan Category:
Mission.
Strategies and goals.
Senior management approval.
Organizational approach to incident response.
How the incident response team will communicate with the rest of the organization and with other organizations.
Metrics for measuring the incident response capability and its effectiveness.
Roadmap for maturing the incident response capability.
How the program fits into the overall organization.
Incident response program structure.
Annual review requirement.

[1] See Appendix VI for a glossary of terms.

9 Elements for the Procedure Category:
Description of specific technical processes used by the incident response team.
Description of techniques used by the incident response team.
Description of checklists used by the incident response team.
Description of forms used by the incident response team.
SOPs should be reasonably comprehensive and detailed to ensure that the priorities of the organization are reflected in response operations.
Standardize responses to minimize errors.
Test SOPs to validate their accuracy and usefulness.
Distribute SOPs to all team members/incident response personnel.
Training SOP users/incident response personnel.
10 Elements for Sharing (Interacting) Information With Outside Parties Category:
The team should document all contacts and communications with outside parties for liability and evidentiary purposes.
The incident handling team should establish media communications procedures that comply with the organization's policies on media interaction and information disclosure.
Conduct training sessions on interacting with the media regarding incidents, which should include the importance of not revealing sensitive information, such as technical details of countermeasures that could assist other attackers, and the positive aspects of communicating important information to the public fully and effectively.
Establish procedures to brief media contacts on the issues and sensitivities regarding a particular incident before discussing it with the media.
Maintain a statement of the current status of the incident so that communications with the media are consistent and up-to-date.
Remind all staff of the general procedures for handling media inquiries.
Hold mock interviews and press conferences during incident handling exercises.
Law enforcement should be contacted through designated individuals in a manner consistent with the requirements of the law and the organization's procedures.
Require Federal agencies to report incidents to the US-CERT.

> Incident handlers should understand how their incident handling actions should differ when a PII breach is suspected to have occurred, such as notifying additional parties or notifying parties within a shorter time frame.

Source: NIST Special Publication 800-61, Security Computer Incident Handling Guide, Rev. 2.

Appendix VI

Glossary of Terms

Term	Definition
Archer System	A commercial off-the-shelf product that provides a web-based application for cyber threat management. The CSIRC captures cybersecurity and computer-related security incidents in the Archer system.
ArcSight	ArcSight is a cybersecurity company designed to help customers identify and prioritize security threats, organize and track incident response activities, and simplify audit and compliance activities.
Botnet	A number of Internet computers that, although their owners are unaware of it, have been set up to forward transmissions (including spam or malware) to other computers on the Internet, usually for the purpose of a cyberattack or denial-of-service attack.
Cybersecurity Incident	Can occur under many circumstances and for many reasons. It can be inadvertent, such as from the loss of an electronic device; deliberate, such as from the theft of a device; or a cyber-based attack by a malicious individual or group, agency insiders, foreign nation, terrorist, or other adversary.
E-mail Attack (Threat Vector)	Can be executed via an e-mail message or attachment. The consequences can include an exploit code disguised as an attached document or a link to a malicious website in the body of an e-mail message.
Ethernet	An array of networking technologies and systems used in local area networks, where computers are connected within a primary physical space. Systems using Ethernet communication divide data streams into packets, which are known as frames. Frames include source and destination address information, as well as mechanisms used to detect errors in transmitted data and retransmission requests.

Term	Definition
External/Removable Media (Threat Vector)	An attack executed from removable media or a peripheral device. A consequence is a malicious code spreading onto a system from an infected flash drive.
Get Transcript Application	Allows taxpayers to view and download their tax information, such as account transactions, line-by-line tax return information, and income reported to the IRS. Taxpayers can download or print five distinct transcript types: tax account, tax return, record of account, wage and income, and verification of nonfiling.
Host-Based Intrusion Detection System	Monitors a computer system to detect an intrusion or violation of the system's security policies and responds by logging the activity and notifying the designated authority. This tool has the ability to monitor key system files and any attempt to overwrite these files.
Improper Usage (Threat Vector)	Any incident resulting from violation of an organization's acceptable usage policies by an authorized user. The consequences can include a user installing file-sharing software, which could lead to the loss of sensitive data, or that a user performs illegal activities on a system.
Internet Protocol Version 4 (IPv4)	The fourth revision of the Internet Protocol and a widely used protocol in data communication over different kinds of networks. IPv4 is a connectionless protocol used in packet-switched layer networks, such as Ethernet.
Internet Protocol Version 6 (IPv6)	The basics of IPv6 are similar to those of IPv4 – devices can use IPv6 as source and destination addresses to pass packets over a network, and tools like ping work for network testing as they do in IPv4, with some slight variations.
Joint Audit Management Enterprise System	The Department of the Treasury system for use by all bureaus to track, monitor, and report the status of internal control audit results. This system tracks specific information on issues, findings, recommendations, and planned corrective actions from audit reports issued by oversight agencies, such as TIGTA.
Loss or Theft of Equipment (Threat Vector)	The loss or theft of a computing device or media used by the organization. A consequence is a misplaced laptop or mobile device containing PII that could be used for financial gain.

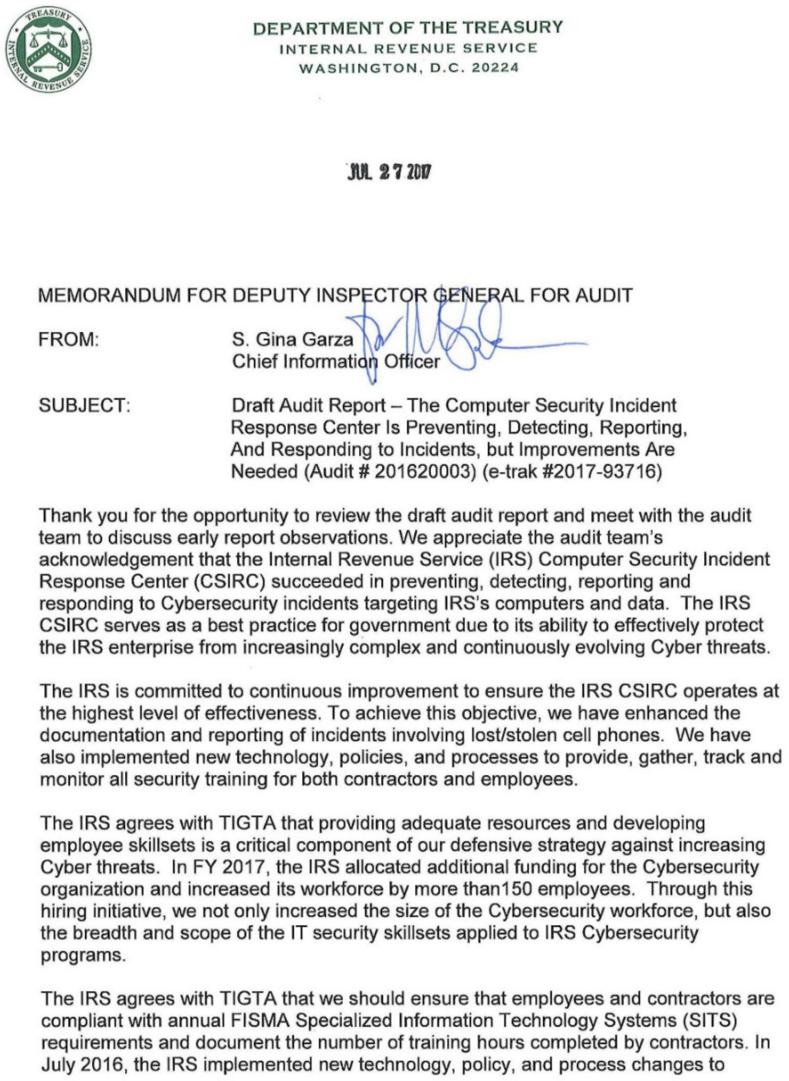
Term	**Definition**
Malware	A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the computer's data, applications, or operating system.
McAfee	A brand that is a part of Intel Security delivering proactive and proven security solutions and services that help secure systems and networks around the world. Intel Security protects consumers and businesses of all sizes from the latest malware and emerging online threats.
National Institute of Standards and Technology	The NIST, under the Department of Commerce, is responsible for developing standards and guidelines for providing adequate information security for all Federal Government agency operations and assets.
Personally Identifiable Information	Information that can be used to distinguish or trace an individual's identity, such as their name, Social Security Number, biometric records, *etc*., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, *etc*.
Skills Framework for the Information Age Standards	A practical resource for people who manage or work in information systems-related roles of any type. It provides a common reference model in a two-dimensional framework consisting of skills and levels of responsibility. It describes professional skills at various levels of competence. It also describes generic levels of responsibility, in terms of Autonomy, Influence, Complexity, and Business Skills.
Sourcefire	A network security company known for its open source network intrusion detection system called Snort. Sourcefire has been subsequently acquired by Cisco.
Symantec	The company produces software for security, storage, backup, and availability - and offers professional services to support its software.
Task Order	An order for services placed against an established contract or with Government sources.

Term	Definition
Tcpdump	A type of packet analyzer software utility that monitors and logs Transmission Control Protocol/Internet Protocol traffic passing between a network and the computer on which it is executed.
Threat Vector	The path or route used by an adversary to gain access to the target. The following threat vectors are used to classify incidents by the method of attack: Attrition Attack, Web Attack, E-Mail Attack, External/Removable Media Attack, Impersonation/Spoofing Attack, Improper Usage, Loss or Theft of Equipment, Unknown Attack, and Other Attack.
United States Computer Emergency Readiness Team	This team acts as the Federal information security incident center for the U.S. Federal Government per the FISMA of 2014.[1]
Web Attack (Threat Vector)	A web attack is executed from a website or web-based application. The consequences can include a cross-site scripting attack used to steal credentials or a redirect to a site that exploits a browser vulnerability and installs malware.
Wireshark	A free and open source network protocol analyzer that enables users to interactively browse the data traffic on a computer network.

[1] Pub. L. No. 113-283.

Appendix VII

Management's Response to the Draft Report



DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

JUL 27 2017

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: S. Gina Garza
Chief Information Officer

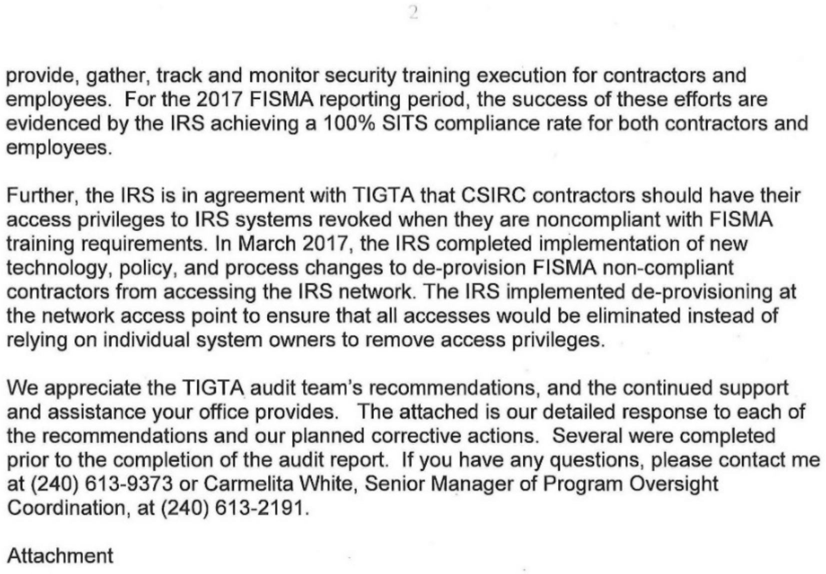
SUBJECT: Draft Audit Report – The Computer Security Incident Response Center Is Preventing, Detecting, Reporting, And Responding to Incidents, but Improvements Are Needed (Audit # 201620003) (e-trak #2017-93716)

Thank you for the opportunity to review the draft audit report and meet with the audit team to discuss early report observations. We appreciate the audit team's acknowledgement that the Internal Revenue Service (IRS) Computer Security Incident Response Center (CSIRC) succeeded in preventing, detecting, reporting and responding to Cybersecurity incidents targeting IRS's computers and data. The IRS CSIRC serves as a best practice for government due to its ability to effectively protect the IRS enterprise from increasingly complex and continuously evolving Cyber threats.

The IRS is committed to continuous improvement to ensure the IRS CSIRC operates at the highest level of effectiveness. To achieve this objective, we have enhanced the documentation and reporting of incidents involving lost/stolen cell phones. We have also implemented new technology, policies, and processes to provide, gather, track and monitor all security training for both contractors and employees.

The IRS agrees with TIGTA that providing adequate resources and developing employee skillsets is a critical component of our defensive strategy against increasing Cyber threats. In FY 2017, the IRS allocated additional funding for the Cybersecurity organization and increased its workforce by more than150 employees. Through this hiring initiative, we not only increased the size of the Cybersecurity workforce, but also the breadth and scope of the IT security skillsets applied to IRS Cybersecurity programs.

The IRS agrees with TIGTA that we should ensure that employees and contractors are compliant with annual FISMA Specialized Information Technology Systems (SITS) requirements and document the number of training hours completed by contractors. In July 2016, the IRS implemented new technology, policy, and process changes to



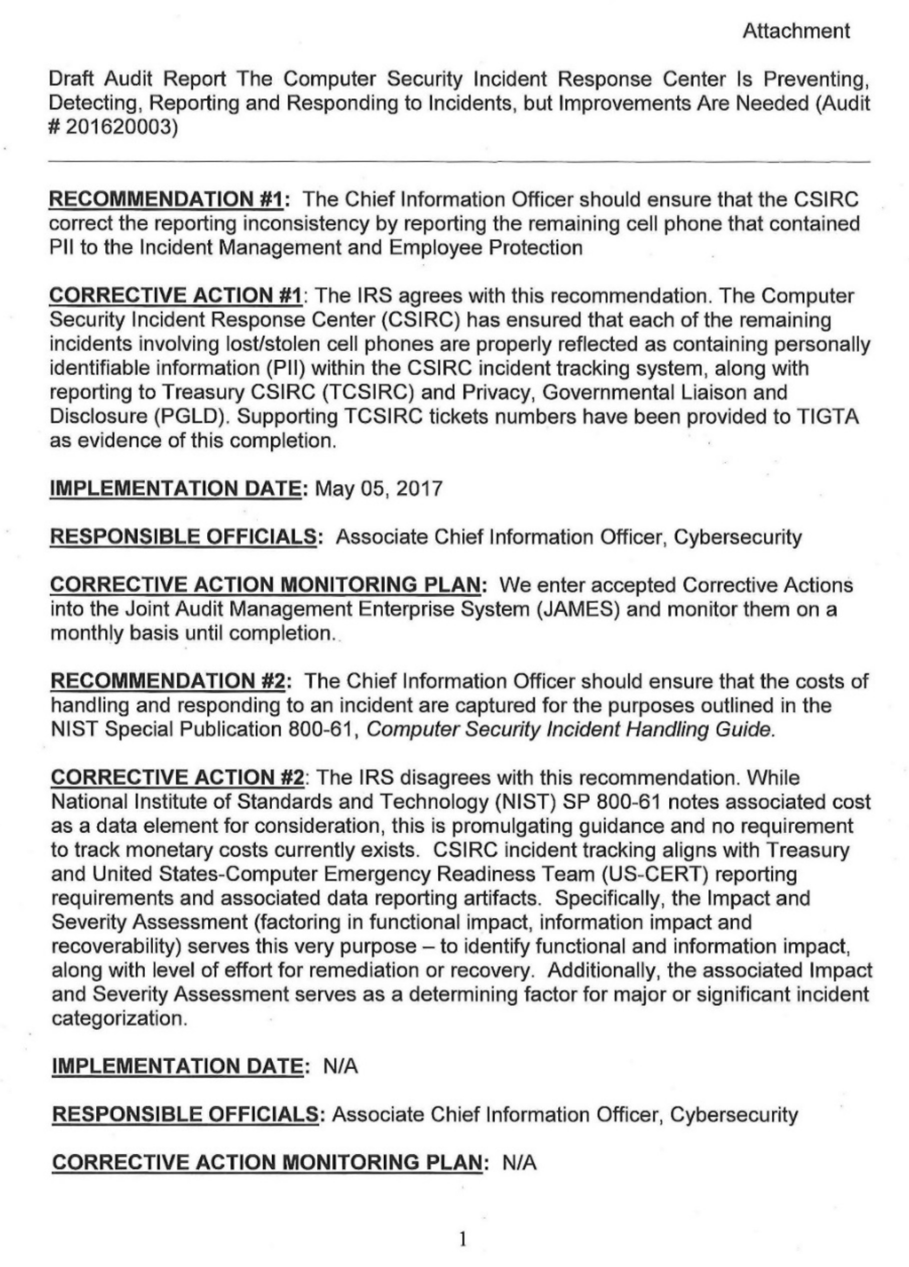
2

provide, gather, track and monitor security training execution for contractors and employees. For the 2017 FISMA reporting period, the success of these efforts are evidenced by the IRS achieving a 100% SITS compliance rate for both contractors and employees.

Further, the IRS is in agreement with TIGTA that CSIRC contractors should have their access privileges to IRS systems revoked when they are noncompliant with FISMA training requirements. In March 2017, the IRS completed implementation of new technology, policy, and process changes to de-provision FISMA non-compliant contractors from accessing the IRS network. The IRS implemented de-provisioning at the network access point to ensure that all accesses would be eliminated instead of relying on individual system owners to remove access privileges.

We appreciate the TIGTA audit team's recommendations, and the continued support and assistance your office provides. The attached is our detailed response to each of the recommendations and our planned corrective actions. Several were completed prior to the completion of the audit report. If you have any questions, please contact me at (240) 613-9373 or Carmelita White, Senior Manager of Program Oversight Coordination, at (240) 613-2191.

Attachment



Attachment

Draft Audit Report The Computer Security Incident Response Center Is Preventing, Detecting, Reporting and Responding to Incidents, but Improvements Are Needed (Audit # 201620003)

RECOMMENDATION #1: The Chief Information Officer should ensure that the CSIRC correct the reporting inconsistency by reporting the remaining cell phone that contained PII to the Incident Management and Employee Protection

CORRECTIVE ACTION #1: The IRS agrees with this recommendation. The Computer Security Incident Response Center (CSIRC) has ensured that each of the remaining incidents involving lost/stolen cell phones are properly reflected as containing personally identifiable information (PII) within the CSIRC incident tracking system, along with reporting to Treasury CSIRC (TCSIRC) and Privacy, Governmental Liaison and Disclosure (PGLD). Supporting TCSIRC tickets numbers have been provided to TIGTA as evidence of this completion.

IMPLEMENTATION DATE: May 05, 2017

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION #2: The Chief Information Officer should ensure that the costs of handling and responding to an incident are captured for the purposes outlined in the NIST Special Publication 800-61, *Computer Security Incident Handling Guide.*

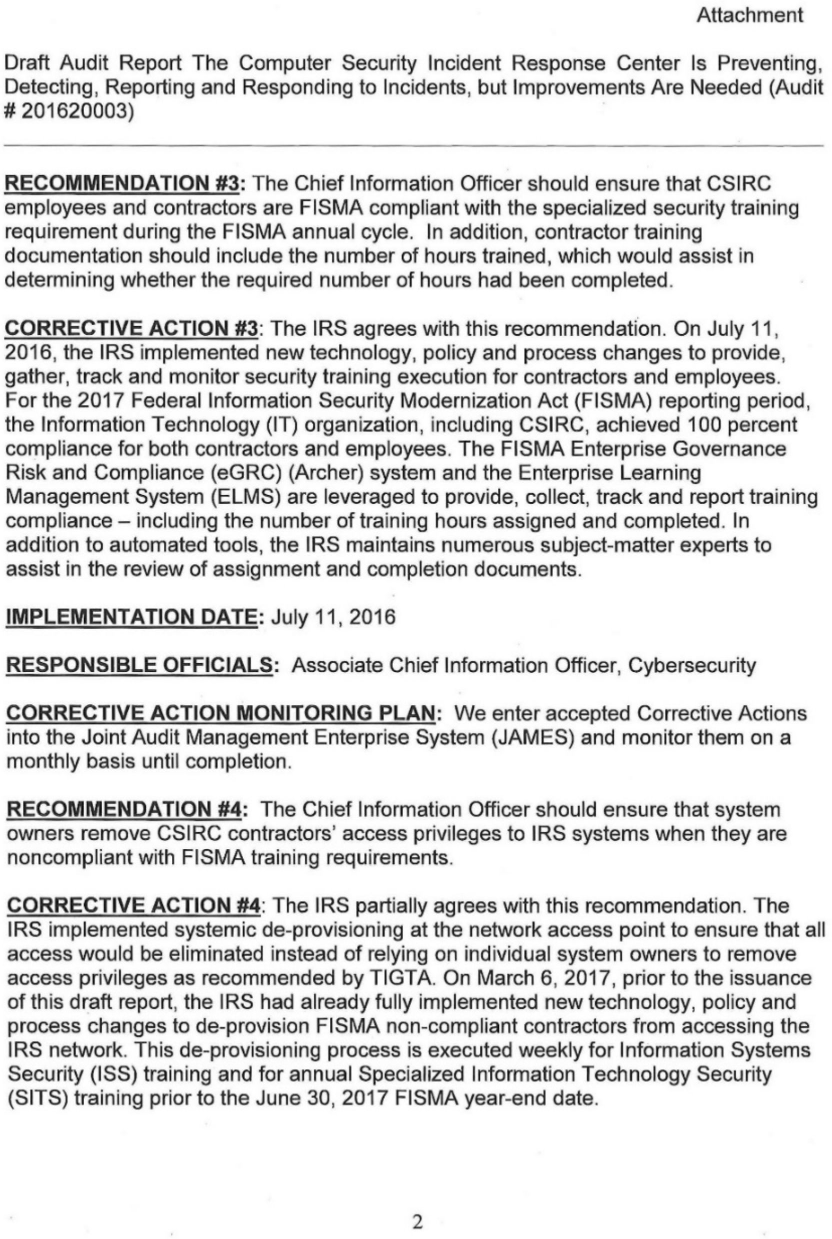
CORRECTIVE ACTION #2: The IRS disagrees with this recommendation. While National Institute of Standards and Technology (NIST) SP 800-61 notes associated cost as a data element for consideration, this is promulgating guidance and no requirement to track monetary costs currently exists. CSIRC incident tracking aligns with Treasury and United States-Computer Emergency Readiness Team (US-CERT) reporting requirements and associated data reporting artifacts. Specifically, the Impact and Severity Assessment (factoring in functional impact, information impact and recoverability) serves this very purpose – to identify functional and information impact, along with level of effort for remediation or recovery. Additionally, the associated Impact and Severity Assessment serves as a determining factor for major or significant incident categorization.

IMPLEMENTATION DATE: N/A

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: N/A

1



Attachment

Draft Audit Report The Computer Security Incident Response Center Is Preventing, Detecting, Reporting and Responding to Incidents, but Improvements Are Needed (Audit # 201620003)

RECOMMENDATION #3: The Chief Information Officer should ensure that CSIRC employees and contractors are FISMA compliant with the specialized security training requirement during the FISMA annual cycle. In addition, contractor training documentation should include the number of hours trained, which would assist in determining whether the required number of hours had been completed.

CORRECTIVE ACTION #3: The IRS agrees with this recommendation. On July 11, 2016, the IRS implemented new technology, policy and process changes to provide, gather, track and monitor security training execution for contractors and employees. For the 2017 Federal Information Security Modernization Act (FISMA) reporting period, the Information Technology (IT) organization, including CSIRC, achieved 100 percent compliance for both contractors and employees. The FISMA Enterprise Governance Risk and Compliance (eGRC) (Archer) system and the Enterprise Learning Management System (ELMS) are leveraged to provide, collect, track and report training compliance – including the number of training hours assigned and completed. In addition to automated tools, the IRS maintains numerous subject-matter experts to assist in the review of assignment and completion documents.

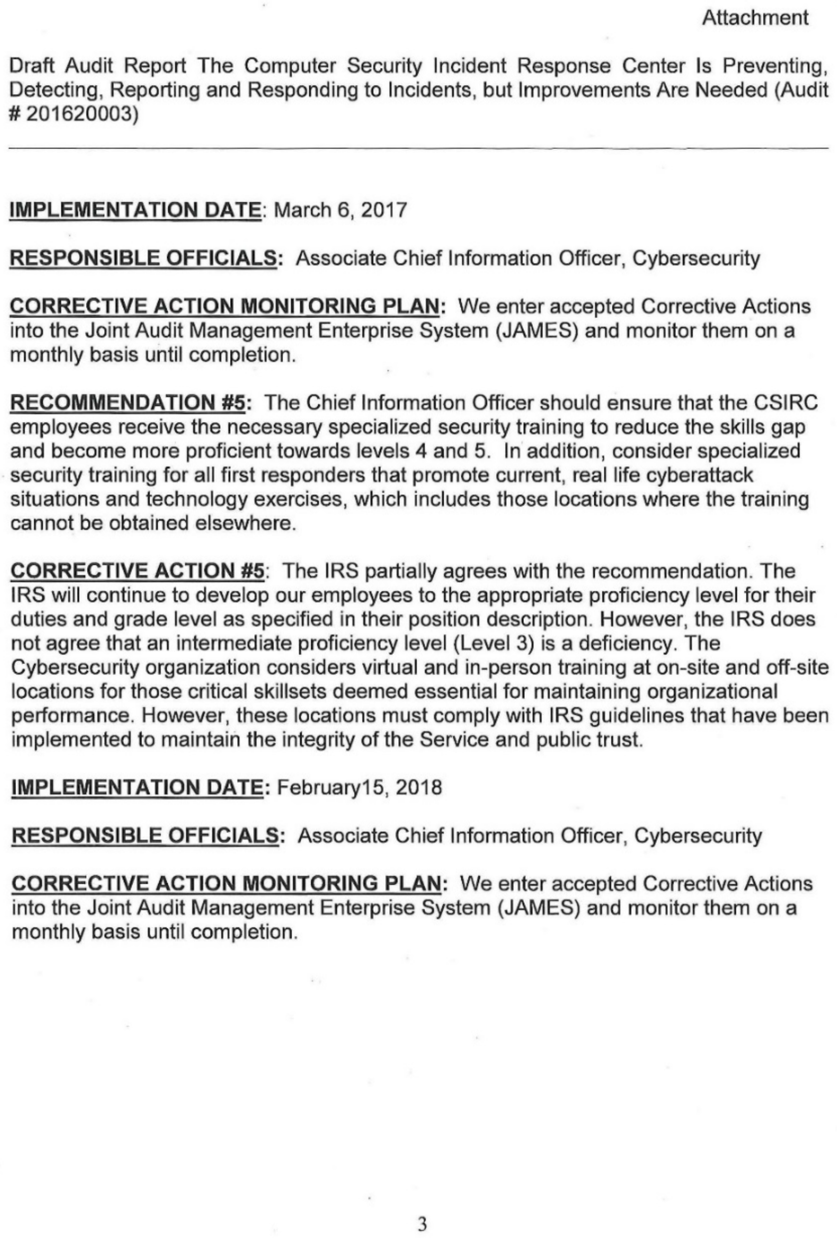
IMPLEMENTATION DATE: July 11, 2016

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION #4: The Chief Information Officer should ensure that system owners remove CSIRC contractors' access privileges to IRS systems when they are noncompliant with FISMA training requirements.

CORRECTIVE ACTION #4: The IRS partially agrees with this recommendation. The IRS implemented systemic de-provisioning at the network access point to ensure that all access would be eliminated instead of relying on individual system owners to remove access privileges as recommended by TIGTA. On March 6, 2017, prior to the issuance of this draft report, the IRS had already fully implemented new technology, policy and process changes to de-provision FISMA non-compliant contractors from accessing the IRS network. This de-provisioning process is executed weekly for Information Systems Security (ISS) training and for annual Specialized Information Technology Security (SITS) training prior to the June 30, 2017 FISMA year-end date.



Attachment

Draft Audit Report The Computer Security Incident Response Center Is Preventing, Detecting, Reporting and Responding to Incidents, but Improvements Are Needed (Audit # 201620003)

IMPLEMENTATION DATE: March 6, 2017

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION #5: The Chief Information Officer should ensure that the CSIRC employees receive the necessary specialized security training to reduce the skills gap and become more proficient towards levels 4 and 5. In addition, consider specialized security training for all first responders that promote current, real life cyberattack situations and technology exercises, which includes those locations where the training cannot be obtained elsewhere.

CORRECTIVE ACTION #5: The IRS partially agrees with the recommendation. The IRS will continue to develop our employees to the appropriate proficiency level for their duties and grade level as specified in their position description. However, the IRS does not agree that an intermediate proficiency level (Level 3) is a deficiency. The Cybersecurity organization considers virtual and in-person training at on-site and off-site locations for those critical skillsets deemed essential for maintaining organizational performance. However, these locations must comply with IRS guidelines that have been implemented to maintain the integrity of the Service and public trust.

IMPLEMENTATION DATE: February15, 2018

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.