



Office of the Inspector General
U.S. Department of Justice

OVERSIGHT ★ INTEGRITY ★ GUIDANCE



**Audit of the Federal Bureau of
Investigation's Cyber Victim
Notification Process**

REDACTED FOR PUBLIC RELEASE

The full version of this report contains information that the Department considered to be classified and therefore could not be publicly released. To create this public version of the report, the Office of the Inspector General redacted (blacked out) portions of the full report.

Audit Division 19-23

March 2019



(U) Executive Summary

(U) Audit of the Federal Bureau of Investigation's Cyber Victim Notification Process

(U) Objective

(U) The objective of this audit was to evaluate the Federal Bureau of Investigation's (FBI) processes and practices for notifying and engaging with victims of cyber intrusions. Specifically, we examined the FBI's adherence to Executive Order 13636, Improving Critical Infrastructure Cybersecurity, and the FBI Cyber Division Policy Guide 0853PG as well as other related policies.

(U) Results in Brief

(U) The FBI established Cyber Guardian for tracking the production, dissemination, and disposition of cyber-victim notifications which can help victims mitigate the damage caused by cyber intrusions and increase the potential for intelligence collection by the FBI. However, we found that the data in Cyber Guardian was incomplete and unreliable, making the FBI unable to determine whether all victims are being notified. The quality of formal requests for investigative actions, called leads, set for victim notification was inconsistent. In addition, not all agents indexed victims within Sentinel, as required. Together, the inconsistent lead and indexing contributed to some notifications not being tracked properly or taking place too long after the attack for the victim to effectively mitigate the threat to its systems. Further, the Department of Homeland Security (DHS)—a partner in using Cyber Guardian—was not entering information into the system as required, contributing to the incompleteness of data in Cyber Guardian. We also found that victims identified in national security cyber cases were not informed of their rights as required by the Attorney General Guidelines for Victim and Witness Assistance (AG Guidelines). The FBI plans to replace Cyber Guardian in fiscal year (FY) 2019 with CyENERGY, a new system which may solve some, but not all data quality issues.

(U) Recommendations

(U) Our report contains 13 recommendations to assist the FBI and the Department of Justice in improving the efficiency and effectiveness of the cyber victim notification process.

(U) Audit Results

(U) **Reliability of Cyber Guardian Data** - We found that the data in Cyber Guardian was unreliable due to typographical errors, a lack of logic controls that would prevent input errors, and incomplete inclusion of victim notifications from restricted access cases.

(U) **Notifying Victims of their Rights under the AG Guidelines** - We found that not all victims were informed of their rights as required by the AG Guidelines. This occurred because: (1) the AG Guidelines are outdated since they do not consider the needs of victims of cybercrime; (2) there is no widely accepted definition of what constitutes a victim of cybercrime; and (3) there is currently no process for getting cybercrime victims' information from national security cases into the FBI's Victim Notification System—the FBI system used to inform crime victims of their rights.

(U) **Quality and Consistency of Leads** - The quality of leads set for victim notification varied depending on the author of the lead and less-detailed leads often made it difficult for agents who are not well-versed in the details of the case to make useful notifications to victims. According to FBI Special Agents experienced with making cyber victim notifications, for a notification to be helpful to a victim, the following information needs to be provided: (1) Internet Protocol addresses affected by the malicious activity; (2) a date or range of dates the activity occurred; (3) any information about the attack that the victim can use to search for the activity in their logs; and (4) in national security cases, a section of unclassified information that can be shared with the victim.

(U) **Victim Engagement** - We met with or received comments from 14 victims to discuss their interactions with the FBI and found that the majority thought highly of the FBI and those interactions. However, some victims complained about the timeliness of the notifications and whether the information provided by the FBI was adequate to remediate the threat to its systems.



(U) Executive Summary

(U) Audit of the Federal Bureau of Investigation's Cyber Victim Notification Process

(U) Coordination with Other Government

Agencies - We found several issues in instances where the FBI coordinates victim notifications with Other Government Agencies. Victim Contact Planning calls, which are interagency conference calls for coordinating initial contact with victims, were not conducted for all cyber incidents that required coordination, first by the Cyber Division Threat Prioritization Matrix, then, beginning in July 2015, by the National Security Council's Cyber Incidents Severity Schema. Also, DHS did not enter the victim notifications that it conducted into Cyber Guardian, contributing to the incompleteness of data in Cyber Guardian. According to DHS, technical constraints contributed to its difficulty entering cyber events into Cyber Guardian. Finally, we found that some notifications were delayed because of the need to protect the identities of victims identified by another government agency.

(U) CyNERGY System to Replace Cyber Guardian -

In FY 2019, the FBI plans to replace Cyber Guardian with a new system called CyNERGY. CyNERGY was still under development at the time of our audit so we were unable to thoroughly evaluate the system and make definitive judgments on its performance. We found that, if the system performs as intended, some of the issues we observed with Cyber Guardian, such as logical input errors, and the ease of making changes to the system should be addressed. However, other concerns will remain without additional fixes, such as the need for CyWatch—an FBI Cyber Division unit that coordinates cyber incident management—to manually input data in the system, and therefore rely on agents to use a specific type of lead category or to index victims properly. In addition, we found that the FBI did not have controls in place to ensure that Cyber Guardian users were up to date with their training for handling Protected Critical Infrastructure Information, which will also be an issue with CyNERGY. Finally, the new system will also reside on the Secret enclave, which will not solve the problem DHS says prevents it from easily entering its data into Cyber Guardian.

**(U) AUDIT OF THE FEDERAL BUREAU OF INVESTIGATION'S
CYBER VICTIM NOTIFICATION PROCESS**

(U) TABLE OF CONTENTS

(U) INTRODUCTION 1

 (U) Background 2

 (U) Executive Order 13636, Improving Critical Infrastructure
 Cybersecurity 2

 (U) Presidential Policy Directive 41, United States Cyber Incident
 Coordination 3

 (U) Agency Incident Response 4

 (U) Attorney General Guidelines for Victim and Witness Assistance .. 4

 (U) Cyber Victim Notification 5

 (U) OIG Audit Approach 8

(U) AUDIT RESULTS 10

 (U) Cyber Guardian System for Tracking Cyber Victim Notifications 11

 (U) Reliability of Cyber Guardian Data 12

 (U) Logical and Typographical Errors 12

 (U) Victim Notification Leads 13

 (U) Indexing Victims in Sentinel 16

 (U) Tracking Victim Notifications in Restricted Access Cases 17

 (U) Notifying Cybercrime Victims of their Rights under the Attorney General
 Guidelines 18

 (U) Quality and Consistency of Leads 20

 (U) Victim Engagement 22

 (U) Coordination with Other Government Agencies 23

 (U) First Look and Victim Contact Planning Call 23

 (U) Cyber Guardian Usage by Agency 24

 (U) Challenges in Notifying Victims Identified by Other Government
 Agencies 27

(U) CyNERGY System to Replace Cyber Guardian 30

(U) CONCLUSION AND RECOMMENDATIONS 34

(U) STATEMENT ON INTERNAL CONTROLS 36

(U) STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS..... 37

(U) APPENDIX 1: OBJECTIVE, SCOPE, AND METHODOLOGY 38

(U) APPENDIX 2: FEDERAL BUREAU OF INVESTIGATION’S RESPONSE TO THE
DRAFT AUDIT REPORT..... 39

(U) APPENDIX 3: OFFICE OF THE DEPUTY ATTORNEY GENERAL’S RESPONSE TO
THE DRAFT AUDIT REPORT 43

(U) APPENDIX 4: OFFICE OF THE INSPECTOR GENERAL ANALYSIS AND SUMMARY
OF ACTIONS NECESSARY TO CLOSE THE REPORT 44

(U) AUDIT OF THE FEDERAL BUREAU OF INVESTIGATION'S CYBER VICTIM NOTIFICATION PROCESS

(U) INTRODUCTION

(U) The Federal Bureau of Investigation's (FBI) Cyber Division (CyD) is responsible for protecting the national security, economic, and information infrastructure of the United States from cyber intrusion activity.¹ To accomplish these responsibilities, CyD shares investigative information with cyber intrusion victims to protect compromised systems, investigates losses and damages, and helps prevent future attacks. In addition, the CyD provides administrative and operational support to the FBI's 56 field offices in all computer intrusion matters. As of January 2018, the FBI had 721 Special Agents dedicated to cyber investigations, including cyber victim notifications.

(U) According to FBI personnel, victims of cyber intrusions are typically identified by the FBI or its partner agencies in the course of their investigative activities.² As a result, many cyber victims, most of which are companies or organizations, are unaware that they are victims of an intrusion until the FBI notifies them.

(U) The goal of the FBI's cyber victim identification and notification process is to mitigate ongoing and future intrusions at targeted entities.³ In addition, the FBI must adhere to the Attorney General Guidelines for Victim and Witness Assistance (AG Guidelines). These AG Guidelines create a mandatory victim notification paradigm that requires federal investigators and prosecutors to identify victims of crime and notify them of the crime, except when the notification would interfere with an ongoing investigation. The CyD Policy Guide extends this requirement further by requiring cyber agents, in coordination with operational stakeholders, to consider victim notification even when it may interfere with an investigation.

¹ (U) A cyber intrusion is an event occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon.

² (U) The Attorney General Guidelines for Victim and Witness Assistance define a victim as a person that has suffered direct physical, emotional, or pecuniary harm as a result of the commission of a crime, including cases where the victim is an institutional entity.

³ (U) Targeted entities include both victims of a cyber-compromise or intrusion and those that may be targeted but have not yet suffered a compromise or intrusion.

(U) Background

(U) Executive Order 13636 on Improving Critical Infrastructure Cybersecurity (E.O. 13636), issued in 2013, and Presidential Policy Directive 41 (PPD-41) United States Cyber Incident Coordination, issued in 2016, have helped establish the FBI's current cyber victim notification responsibilities. The CyD's strategic objective is to proactively identify, pursue, and defeat cyber threat perpetrators while protecting the freedom, privacy, and civil liberties of U.S. persons. The nature of technology, including the internet, further demands that the FBI approach each cyber threat through coordinated partnerships with government agencies. Victim notification is a compelling way for the CyD to contribute to network defense for the protection of individual, commercial, and government users of the internet, as well as for the protection of the infrastructure itself. It is CyD's policy to notify and disseminate meaningful information to victims and the computer network defense community in a timely manner to the extent to which it does not interfere with ongoing law enforcement or U.S. Intelligence Community investigations, operations, methods, sources, or technologies.

(U//FOUO) In a computer intrusion investigation, the victim that receives notification is the individual, organization, or corporation that is the owner or operator of the computer at the point of compromise. Victims are identified, to the extent possible, by the FBI and its partner agencies during investigations of suspected cybercrimes and cyber-related threats. Without appropriate notification, victims may be unaware they have suffered an intrusion and may not take steps to limit or mitigate the damage done by the intrusion and strengthen their cyber defenses.

[REDACTED] In addition to the FBI CyD Policy Guide, other presidential directives have added to the FBI's responsibilities in cyber victim notification.

(U) Executive Order 13636, Improving Critical Infrastructure Cybersecurity

(U) Coordination between the FBI and its partner agencies is critical for timely and efficient notification of cyber victims. E.O. 13636 addressed the need for such cooperation and mandated steps to improve the process.

(S//NF) With regard to cyber victims, E.O. 13636, Section 4(b) required the establishment of a system for tracking the production, dissemination, and disposition of cyber incidents. The National Security Council required the National Cyber Investigative Joint Task Force (NCIJTF) to lead the development and

implementation of the required system.⁴

[REDACTED]

As of December 2017, over 16,000 cyber events and over 20,000 victim notifications were included in Cyber Guardian. Cyber Guardian is managed by the NCIJTF's CyWatch Unit, the FBI's 24-hour command center for coordinating:

- domestic law enforcement response to criminal and national security cyber intrusions,
- targeted entity notifications, and
- cyber incident management.

(U) According to the FBI, Cyber Guardian was a temporary solution designed to quickly comply with the mandate contained in E.O. 13636, Section 4(b). The FBI is currently developing a system called CyNERGY to replace Cyber Guardian.

(U) Presidential Policy Directive 41, United States Cyber Incident Coordination

(U) PPD-41 proscribes policy for U.S. cyber incident coordination. PPD-41 sets forth the principles governing the federal government's response to any cyber incident, whether involving government or private sector entities. For significant cyber incidents, PPD-41 establishes lead federal agencies and an architecture for coordinating the broader federal government response. PPD-41 also requires the Department of Justice and the Department of Homeland Security (DHS) to maintain

⁴ (U) The NCIJTF was established to serve as the national focal point for the U.S. government's coordination, integration, and information sharing to support cyber threat investigations, supply and support intelligence analysis for community decision-makers, and provide value to other ongoing efforts in the fight against the cyber threat to the nation. National Security Presidential Directive-54/Homeland Security Presidential Directive-23, signed on January 8, 2008, directed the creation of the NCIJTF and appointed the FBI as the lead agency.

⁵ (S//NF)

[REDACTED]

updated contact information for public use to assist entities affected by cyber incidents in reporting those incidents.

(U) Agency Incident Response

(U) For significant cyber incidents, the Department of Justice, acting through the FBI, is designated as the lead agency for threat response activities, because significant cyber events often involve the possibility of a nation-state actor or have some national security nexus.⁶ Threat response activities include conducting appropriate law enforcement and national security investigative activity at the affected entity's site; collecting evidence and gathering intelligence; providing attribution; linking related incidents; identifying additional affected entities; identifying threat pursuit and disruption opportunities; developing and executing courses of action to mitigate the immediate threat; and facilitating information sharing and operational coordination with asset response. DHS is designated as the lead federal agency for asset response activities, which include furnishing technical assistance to affected entities to protect their assets, mitigate vulnerabilities, and reduce impacts of cyber incidents.

(U) Attorney General Guidelines for Victim and Witness Assistance

(U) The AG Guidelines establish guidelines to be followed by Department of Justice personnel in the treatment of victims of and witnesses to crime and apply to all personnel who are engaged in or support investigative, prosecutorial, correctional, or parole functions within the criminal justice system. The Victims' Rights and Restitution Act (VRRRA), 42 U.S.C. § 10607 (2006), and the Crime Victims' Rights Act (CVRA), 18 U.S.C. § 3771 (2006 & Supp. III 2009) are the laws that form the foundation of the AG Guidelines.⁷

(U) Department personnel are required by law and under the AG Guidelines to identify victims of a crime, notify them of their rights, and offer them services as described in the AG Guidelines. Victims, however, are not required to exercise their rights or to accept these services and may choose at any point in the criminal justice process to decline to receive further services or exercise their rights.

⁶ (U) A significant cyber incident is a cyber-incident that is—or group of related cyber incidents that together are—likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.

⁷ (U) The Attorney General Guidelines refer to the Victims' Rights and Restitution Act, 42 U.S.C. § 10607, however that law was subsequently reclassified as section 20141 of Title 34, Crime Control and Law Enforcement.

(U) Cyber Victim Notification

(U//FOUO) The CyD Policy Guide details when victim notifications should be conducted. Victim notifications can originate based on several sources of victim information: victim self-reporting, [REDACTED], shared partner-agency intelligence, or through FBI investigations or intelligence collection. Once CyWatch receives information indicating that an entity has been victimized, the FBI determines the severity of the threat, and labels the incident based on the National Security Council's Cyber Incident Severity Schema. The schema, which is shown below, provides a general definition of each level of severity and handling precedence for interagency coordination and targeted entity contact.

^a (U//FOUO) [REDACTED]

(U//FOUO) Figure 1
National Security Council's Cyber Incident Severity Schema

General Definition	
Level 5 <i>Emergency</i> (Black)	<i>Poses an imminent threat to the provision of wide-scale critical infrastructure services, national gov't stability, or to the lives of U.S. persons.</i>
Level 4 <i>Severe</i> (Red)	<i>Likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties.</i>
Level 3 <i>High</i> (Orange)	<i>Likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.</i>
Level 2 <i>Medium</i> (Yellow)	<i>May impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.</i>
Level 1 <i>Low</i> (Green)	<i>Unlikely to impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.</i>
Level 0 <i>Baseline</i> (White)	Unsubstantiated or Inconsequential event.

(U) Source: FBI

(S//NF)

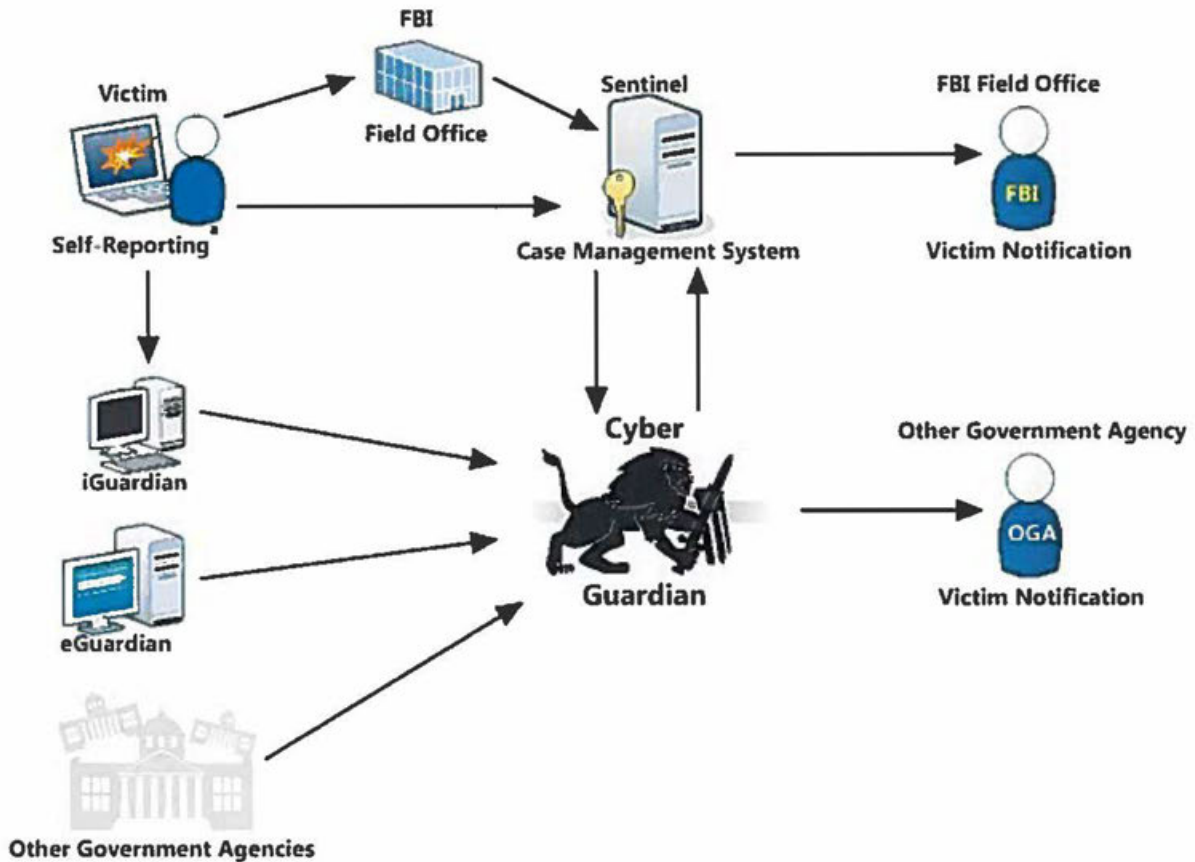
[REDACTED]

(U) Once an incident is labeled, CyWatch creates a lead in Sentinel, the FBI's case management system, and sends the lead to the appropriate Threat Manager.¹⁰ The Threat Manager reviews the information provided by the intelligence report and determines whether to notify the victim. After CyWatch receives notification approval from the Threat Manager, CyWatch sends a new Sentinel lead to the field office (FO) that covers the territory where the victim is located. When the FO receives the lead, it conducts the victim notification. Contact with the victim is made in one of three ways: (1) in person, (2) via phone call, or (3) through email. Unless the FO has a prior relationship with the victim, most of which are companies or organizations, agents prefer to conduct the notification in person. When contact is made with the victim, the victim is under no obligation to cooperate with the FBI unless a subpoena or legal process has been issued. Without improperly disclosing classified information, the FBI will provide as much information as possible to the victim to allow the victim to mitigate the threat. The FBI often asks the victim for permission to monitor the victim's system(s) to observe the adversary's activity and for the victim to provide activity logs for the affected systems.

⁹ (U) The CyTRACKer is an annual report that highlights computer intrusion trends across critical infrastructure sectors, including commercial, transportation, financial services, healthcare, defense, communications, and a host of other areas.

¹⁰ (U) Sentinel provides electronic management of cases, records, tasks, workflow, and items collected as evidence. A lead is a request for work to be done. A lead may require action by the receiver or it may simply be for the purpose of transmitting information. In either case, once the work is complete, the lead is marked covered. A lead may be sent to one or more receiving parties which Sentinel refers to as locations. When a "location" receives a lead, it is assigned to a person to cover. Threat Managers are GS-14 supervisors at CyD Headquarters that manage and coordinate the operational aspects for a specific threat.

**(U) Figure 2
Cyber Victim Notification Process**



^a (U) Victims can self-report cyber incidents through iGuardian which feeds into Cyber Guardian, or through the public access line which is documented in Sentinel, or they can report incidents directly to their local FBI field office.

(U) Source: OIG Review of FBI Data

(U) OIG Audit Approach

(U) The objective of this audit was to evaluate the FBI's processes and practices for notifying and engaging with victims of cyber intrusions. Specifically, we examined the FBI's adherence to E.O. 13636, Improving Critical Infrastructure Cybersecurity; Presidential Policy Directive 41, United States Cybersecurity Incident Coordination; and the FBI CyD Policy Guide 0853PG, dated February 14 2017, as well as other related policies. Our audit focused on the period following November 2014, when Cyber Guardian was first used to satisfy the requirements of E.O. 13636 Section 4(b).

(U) To accomplish our objective, we interviewed FBI officials and conducted fieldwork at FBI Headquarters in Washington, D.C. and several FBI field offices including: Washington, Boston, New Haven, Philadelphia, Chicago, and Baltimore. We also met with personnel from the NSA and DHS. In addition, we met with 14 organizations that received victim notifications from the FBI to discuss those interactions. The scope of our audit generally covered cyber victim notification activity from November 2014 to December 2017 (approximately 20,000 Cyber Guardian entries). Additional information about our approach to this audit can be found in Appendix 1.

(U) AUDIT RESULTS

(U) The FBI established Cyber Guardian to track the production, dissemination, and disposition of cyber victim notifications; however, we found the data within Cyber Guardian is incomplete and unreliable due to: (1) logical and typographical errors, (2) agents not setting leads properly, (3) agents not indexing victims within the automated case management system—Sentinel—as required, and (4) victim notifications linked to cases with restricted access in Sentinel not being tracked in Cyber Guardian. Additionally, we found that in response to the Attorney General Guidelines, the Victim Services Division sends victim notification letters to victims in criminal cyber-cases, but not to victims in cyber-related national security cases, resulting in many victims that are not informed of their rights as required by the Attorney General Guidelines for Victim and Witness Assistance.

(U) We also found that that the amount of information and instructions for leads, which are used to assign tasks to agents such as victim notifications, varied depending on the author of the leads. Leads that contained little detail often made it difficult for agents conducting the notifications to make useful notifications to victims. Similarly, we found that the timeliness and quality of cyber victim notifications affected victims' satisfaction with the process. Seven of the 14 victims we met with said that they had received at least 1 notification too late, or without enough detail, to allow any meaningful remediation to be made. At both FBI headquarters and field offices, FBI cyber personnel acknowledged the timeliness of notifications is a problem. With regard to quality, due to national security classification, the FBI cannot always share sufficient information to allow victims to take action to defend their networks or systems. Victims and FBI Special Agents we interviewed told us that some cyber threat information is classified, limiting the FBI's ability to provide victims with timely and actionable information. Some Special Agents said they had to have the classification of certain information downgraded so it could be made available to a victim.

(U) Other Government Agencies (OGA) within the Federal Cybersecurity Centers are required to utilize Cyber Guardian and update information appropriately.¹¹ We found the FBI enters the vast majority of incidents in Cyber Guardian; however, through our analysis it appears that DHS does not document the majority of the victim notifications it conducts in Cyber Guardian. Without complete cyber victim data, the FBI cannot determine whether all victims are being notified, potentially making victims poorly positioned to defend themselves against cyber threats. The FBI stated that Cyber Guardian would be a much more useful

¹¹ (U) The Federal Cybersecurity Centers include the Defense Cyber Crime Center, the Intelligence Community Security Coordination Center, the National Cybersecurity and Communications Integration Center, the National Cyber Investigative Joint Task Force/CyWatch, the National Security Agency/Central Security Service National Cyber Threat Operations Center, and the United States Cyber Command Joint Operations Center.

tool if DHS entered all of its victim notification information, reducing the risk of duplicate victim notifications and identifying trends in current and emerging cyber threats. As described in more detail later in the report, DHS stated that technical constraints make it difficult for DHS to enter cyber events into Cyber Guardian. Finally, we found that the FBI did not have controls in place to ensure that Cyber Guardian users were up to date with their training for handling Protected Critical Infrastructure Information.

(U) Cyber Guardian System for Tracking Cyber Victim Notifications

(U) In response to E.O. 13636, Improving Critical Infrastructure Cybersecurity Section 4(b), the FBI established the Guardian Victim Analysis Unit and assigned it the responsibility creating a system for cyber victim tracking. The FBI created Guardian for Cyber in response to E.O. 13636 Section 4(b), and relied on the same code as the Counterterrorism Division's (CTD) Guardian system because it had the capability to transfer data between unclassified and classified systems or networks. However, the FBI found that operating a CyD system within the confines of a system built for CTD cases presented challenges, such as having to rely on CTD to make changes to the system because CyD personnel did not have authority to make changes to the system. Therefore, in November 2014, Cyber Guardian was developed as a separate system, and the data from Guardian for Cyber was manually transferred over to the new system. At the time of our audit, CTD Guardian and Cyber Guardian continued to share the same infrastructure, and Cyber Guardian continues to rely on CTD Guardian system developers for changes and upgrades.

(U//FOUO) Before September 2018, Cyber Guardian automatically ingested information at the unclassified level from iGuardian and InfraGard, and Law Enforcement Sensitive information from eGuardian.¹² Subsequent to our fieldwork on this audit, the FBI told us that in September 2018 it changed the way cyber threat events from iGuardian and eGuardian were handled, routing them to the field offices through CTD Guardian rather than to CyWatch through Cyber Guardian. Additionally, Cyber Guardian ingests information from the FBI's case management system, Sentinel, and [REDACTED] at the Secret level.

¹² (U) iGuardian is a platform through which the FBI's law enforcement partners provide potential terrorism-related threats and suspicious activity reports. InfraGard is a partnership between the FBI and the private sector. It is an association of persons who represent businesses, academia, state and local law enforcement agencies, and others dedicated to sharing information and intelligence to prevent hostile acts against the United States. The eGuardian system collects and shares terrorism-related activities amongst law enforcement agencies across various jurisdictions. The information captured in eGuardian is also migrated to the FBI's Internal Guardian system.

(U) The FBI and its NCIJTF partners use Cyber Guardian to manage and coordinate victim information. The system is maintained by CyWatch on the FBI's Secret network.¹³ CyWatch provided us with a data export from Cyber Guardian which showed the Targeted Entities and Cyber Incidents in Cyber Guardian as of December 2017. According to the data, as of December 2017, Cyber Guardian had 16,409 cyber incidents and 20,803 victim notifications, including older incidents transferred from previous databases.

(U) Reviewing the data provided, we found that the information on cyber events in Cyber Guardian includes, but is not limited to, the:

- targeted entity's name,¹⁴
- serial number to identify the incident,
- statuses of the incident and the notification,
- date and time of the notification, if one was made,
- priority level,
- threat actor type,
- agency that identified the event and targeted entity, and
- agency that conducted the victim notification, if one was made.

(U) Reliability of Cyber Guardian Data

(U) We could not completely assess the notification process and determine whether victims were notified timely because, during our audit, we identified missing and inaccurate data. Specifically, our review found issues with Cyber Guardian data including: logical and typographical errors, incorrect types of leads used in Sentinel, incorrect indexing of victims in Sentinel, and data from restricted cases not being entered into Cyber Guardian. These issues are discussed in greater detail below.

(U) Logical and Typographical Errors

(U) We reviewed notification data from Cyber Guardian and found several issues with the quality of the data. For example, we found errors with at least 61 notifications which, according to the data in Cyber Guardian, took place before the incident was observed by the reporting agency.¹⁵ In these examples, the "Date/Time Notified" was a date earlier than the "Incident Observed Date/Time." We also found typographical errors related to the manual entry of data into the

¹³ (U) The Guardian Victim Analysis Unit was incorporated into the CyWatch Unit at the NCIJTF.

¹⁴ (U) Within CyD investigations, it is not always clear whether an entity was victimized or simply targeted by a threat actor, therefore CyD uses the term "Targeted Entity" within Cyber Guardian.

¹⁵ (U) The reporting agency can be any of the member agencies of the NCIJTF.

system. Specifically, we found instances in which victim identifiers, such as names of entities, cities, and states, were spelled incorrectly. Similarly, some entities were entered with many variations, for example, "U.S. Air Force," "US Air Force," or "U.S. Department of the Air Force." Typographical spelling errors and name variations can potentially cause problems with duplicate notifications if a Cyber Guardian user searches for notifications made to a specific company or organization and finds no records in the system because the entity's name was misspelled or inconsistently entered. Further, these errors reduce confidence in the reliability of the data contained within Cyber Guardian.

(U) We discussed these issues with CyWatch officials and they acknowledged that data input errors are a concern. Those officials said that Cyber Guardian does not have controls that would prevent users from inputting dates that do not make logical sense, such as notifications that occur prior to a cyber-incident being detected. They also stated that many errors were due to the manual effort to transfer data from the original Guardian for Cyber system into the newer Cyber Guardian system. Because the accuracy of the data housed in Cyber Guardian is critical to coordinating the Government's response to cyber incidents as directed by E.O. 13636, we recommend that the FBI ensures there are appropriate logic controls for data that are manually input into Cyber Guardian and CyNERGY, and that CyNERGY's data input is as automated as appropriate.

(U) Victim Notification Leads

(U) Sentinel includes a lead function with a primary purpose to allow investigative work to be assigned to other units or field offices. As it relates to victim notification, an agent can identify a victim of a cybercrime in another area and set a lead in Sentinel requesting that the victim be notified by an agent in the field office responsible for the area in which the victim is located. There are different types of leads that can be set in Sentinel, including:

- Information Only,
- Action, and
- Victim Notification.

(U) In an effort to ensure all victim notifications are captured in Cyber Guardian, CyWatch relies on a team of six contractors dedicated to quality assurance and data input who manually search Sentinel daily for victim notifications requested through "Action" leads, and if found, manually enter those notifications into Cyber Guardian. However, when agents set leads as "Victim Notification" leads, those leads are flagged for CyWatch contractors to enter into Cyber Guardian.

(U) "Victim Notification" leads were added to Sentinel as part of a 2013 update. In 2014, the FBI's CyD convened a Guardian for Cyber Focus Group (focus group) to evaluate the cyber victim notification process. The focus group discussed

impediments to cyber victim notifications and possible solutions to those impediments. The focus group concluded that it was burdensome to require agents in the field to enter victim information into both Sentinel and Cyber Guardian. Based on the focus group's conclusions, the CyD's Assistant Director directed field agents to only use Sentinel and made CyWatch responsible for ensuring that data is transferred between the two systems. The focus group also detailed the importance of proper data entry into Sentinel to ensure the information gets captured in Cyber Guardian. Two factors highlighted by the focus group to achieve improvements included that victims must be indexed as "victims" in Sentinel, and that leads for victim notification must use the "Victim Notification" lead type, not "Action" leads. Additionally, five "Lync and Learn" training sessions were provided to CyD personnel to inform agents on the proper way to use Sentinel for documenting cyber incidents and victim notifications. However, these training sessions were a one-time offering and were not mandatory.

(U) During this audit, we visited six FBI field offices and discussed the victim notification process with cyber squad Special Agents and supervisory Special Agents. In our discussions, we found that 29 of 31 field agents we interviewed do not use the "Victim Notification" lead type when setting leads for victim notification. Five of the agents had not even heard of it. The agents with whom we spoke stated that they primarily used "Action" leads when requesting other field offices to conduct a victim notification and that the leads they receive for cyber victim notifications are also typically "Action" leads. In response to our raising this point, CyWatch said it believes that some agents are not sure which type of lead to use when multiple tasks are requested in the same lead, including victim notification and other strictly investigative tasks.

(S//NF) [REDACTED]

¹⁶ (S//NF) [REDACTED]

¹⁷ (U) We determined this by reading the leads and associated Sentinel documentation and looking for key words and phrases such as, "Please notify [person/organization] that they may have been targeted by a spear phishing campaign." Some were not obvious, but we used our professional judgment to determine whether or not the lead was for a victim notification.

[REDACTED]

(S//NF)

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

(S//NF)

[REDACTED]

(U) In another example, the victim's identity at the time of the intrusion was different than when the notification was made due to one company acquiring the other. The supporting documentation from Sentinel had the company's original name, but the new name was used for the record in Cyber Guardian. This again illustrates data accuracy issues that must be considered for Cyber Guardian users.

¹⁸ (S//NF)

[REDACTED]

(U) We also found one notification that should have been in Cyber Guardian, and upon further research after we raised this concern, CyWatch discovered that several notifications found through a daily search of Sentinel were not transferred into Cyber Guardian. The reason for this was unclear, but this discovery highlights the risk of the manual search of Sentinel for victim notifications. This risk could be mitigated by increasing the automation of data entry into Cyber Guardian.

(U) Finally, a victim was notified by the FBI in one instance, but the notification was entered into Cyber Guardian under his employer's name. These examples show why the quality of the data in the system is important for users who want to check the system to determine whether a victim has already been informed prior to making a notification.

(U) Using "Action" leads to request victim notifications increases the risk that notifications are not tracked in Cyber Guardian as required by E.O. 13636 and increases the chance of duplicate notifications by another agency that cannot see that the victim was already notified. According to the FBI, duplicate notifications may damage the FBI's relationship with the private sector by making the Government appear unprofessional and disorganized, and those relationships are essential for information and intelligence sharing. In addition, agents have expressed concerns that another agency conducting a duplicate notification could spook a cooperating victim that agreed to consensual monitoring, or compromise ongoing Foreign Intelligence Surveillance Act collections, thereby jeopardizing sensitive intelligence collection.¹⁹ Therefore, we recommend that the FBI strengthen controls for ensuring that victim notifications are tracked in Cyber Guardian, to include agents using "Victim Notification" leads in Sentinel as required by CyD Policy Guide 0853PG.

(U) Indexing Victims in Sentinel

(U) In addition to using Victim Notification leads in Sentinel, it is also important that victims are correctly indexed as "Victims" in Sentinel. Indexing is a function in Sentinel that allows agents to connect entities and attributes within the case management system. For example, if an agent indexes John Doe as a "Victim" and associates an Internet Protocol (IP) address, a particular threat actor, and a method of attack used against that person, it will allow agents in other cases to discover potential connections between cases. Further, for victim notification tracking, indexing an entity as a "Victim" allows CyWatch to find and manually transfer victim notification information from Sentinel to Cyber Guardian. CyWatch searches Sentinel for recently indexed victims that are associated with cyber cases.

¹⁹ (U) Consensual monitoring is when a victim voluntarily agrees to let the FBI monitor the activity on the victim's systems to gather evidence of illicit activity by the cyber threat actor.

(S//NF) Using a risk based approach we selected a National Security Cyber case (Cyber Case A) to determine how entities were indexed in Sentinel. We identified ██████████ indexed in Cyber Case A and showed ██████████ (99 percent) were indexed as "References" ██████████ (1 percent) were indexed as "Victims." Because there were so few victims indexed in this case, we were concerned that victim notifications made in this case were not tracked in Cyber Guardian. To address our concerns, we reviewed ██████████ from the case—accounting for approximately 30 percent of the entities indexed and found ██████████ incorrectly indexed as references. Of those ██████████, the Sentinel documentation showed that ██████████ notified. We were only able to ██████████ (34 percent) of the notifications listed in Cyber Guardian. CyWatch confirmed that the ██████████ (66 percent) victim notifications were not in Cyber Guardian. These notifications dated back to 2014, during the transition between Guardian for Cyber and Cyber Guardian. According to CyWatch, notifications associated with National Security cases were not fully entered into Cyber Guardian until the end of 2015 as the initial focus was on criminal cyber intrusion cases.

(U) Cyber Guardian relies on agents properly indexing victims in Sentinel in order to capture all victim notifications. Therefore, we recommend that the FBI ensures that agents index "Victims" in Sentinel as required by the Indexing User Manual for Sentinel to support FBI investigative and administrative matters.

(U) Tracking Victim Notifications in Restricted Access Cases

(U) An especially sensitive case can have access to its Sentinel case file restricted with approval of the division's Assistant Director. A case's files can be restricted when the investigation involves the protection of sources whose lives are at risk, or unauthorized disclosure of the subject of the investigation or intelligence topic creates substantial and serious risk. Details of restricted cases can only be viewed by the agents investigating the case, their chain of command, and other personnel specifically provided with access. Sentinel users that search the system may find results from restricted cases, but the details will be masked.

(U//FOUO) CyWatch demonstrated for us the restricted case capability using one of the multiple restricted cyber-intrusion cases related to one of the victims with whom we spoke. The results of a search of the case number in Sentinel returned a list of documents in the case file, but when the files were opened, all of the text was replaced with "Xs."²⁰ This sample case involved multiple victims. Some of the victim notifications from this case appeared in Cyber Guardian; this

²⁰ (U) Restricted cases can also be set up so that if a Sentinel user searches for names or other details of a restricted case, no search results are returned, but the case agent is notified that someone was searching for details of that case.

occurred when the victim was identified through [REDACTED] that was sent directly to CyWatch.²¹ As anticipated, CyWatch confirmed that only a few of the notifications from our sample case were in Cyber Guardian. All of those notifications resolved back to one or more restricted cases, including our sample case.

(U//FOUO) As with non-restricted cases, victim notifications are automatically entered into Cyber Guardian if the agent sets the leads in Sentinel as "Victim Notification" leads or if the victims were identified [REDACTED]. However, unlike non-restricted cases, when CyWatch conducts its daily review of Sentinel for victim notifications that were not automatically included in Cyber Guardian, it can only see that a notification was conducted for a restricted case; CyWatch cannot view any of the pertinent information necessary to create a Cyber Guardian entry such as the name of the victim or any details of the threat. Although we did not determine the number of cyber victim notifications associated with restricted cases, we found evidence that suggested this issue may be significant. Victim notifications from restricted cases not being entered in Cyber Guardian increases the risk of a U.S. Government agency conducting a duplicate notification to a victim and possibly compromising an ongoing FBI investigation or intelligence collection operation. Therefore, we recommend that the FBI ensure that all cyber victim notifications conducted in the course of restricted investigations are appropriately tracked in Cyber Guardian.

(U) Notifying Cybercrime Victims of their Rights under the Attorney General Guidelines

(U) In addition to improving the accuracy of Cyber Guardian, indexing victims of cybercrime as "Victims" in Sentinel also has an effect on whether the victims are notified of their rights as required by law. When entities in Sentinel are indexed as victims, Victim Specialists, who fall under the purview of the FBI's Office of Victim Assistance (OVA) within the Victim Services Division, begin the process of informing victims of their rights. The AG Guidelines apply to all personnel in the Department of Justice who are engaged in or support investigative, prosecutorial, correctional, or parole functions within the criminal justice system.²² Department personnel are required to identify victims of a crime, notify them of their rights, and

²¹ (U//FOUO) [REDACTED]

²² (U) The Attorney General Guidelines for Victim and Witness Assistance are based on the *Victims' Rights and Restitution Act of 2006*, and the *Crime Victims' Rights Act of 2006* (supplemented in 2009).

offer them services as described in the AG Guidelines.²³ According to the OVA, the primary methodology for notifying cyber victims of their rights is by letter. However, two agents that we met with at two different field offices stated that they were aware of agents not indexing victims in Sentinel as "Victims" because those agents do not want the victim to receive the OVA notification. An agent told us that he does not index victims in Sentinel because he is afraid that the letter will jeopardize fragile agreements with the victims to allow consensual monitoring of their systems. This agent said that it is sometimes difficult to persuade a victim to agree to consensual monitoring and that monitoring provides valuable intelligence.

(U) For Cyber Case A, discussed previously in the Indexing Victims in Sentinel section of this report, we sent to OVA all 44 victim notifications we identified in that case to determine whether those victims received victim notification letters or were notified of their rights under the AG Guidelines in any other way. OVA informed us that none of the 44 victims received notification from OVA. OVA stated that it does not send out victim notification letters to victims identified in national security cyber cases; it only sends notification letters to victims in criminal cyber cases with a 288A case classification code, which is the designation for criminal cyber intrusion cases.

(U) To track the status of the victim notifications, the OVA uses the Victim Notification System, an unclassified system used by the Department and other components that provides important information to victims.²⁴ Criminal cyber cases in the 288A classification code, which contain only unclassified information, are automatically entered into the Victim Notification System from Sentinel. However, since much of the information in national security cyber cases is classified, the Victim Notification System does not automatically ingest information from national security cases. There are only two ways that a victim from a national security cyber investigation would receive a victim notification letter: (1) if an FBI cyber agent received a "Victim Notification" lead, covered the lead and documented the notification in an unclassified electronic communication which was referenced to a 288A administrative case file; or (2) if a cyber-agent specifically asked a victim specialist to send a letter to a specific victim. The OVA acknowledged that both scenarios are unlikely. In fact, according to OVA personnel, they searched the Victim Notification System and found information from only one national security cyber case. OVA personnel stated that even that one case should not have made it

²³ (U) Victims, however, are not required to exercise their rights or to accept these services and may choose at any point in the criminal justice process to decline to receive further services or exercise their rights. Investigators are given latitude to not make notifications if it would negatively affect the investigation; however, if the victims have been notified of the fact that they were victimized, it should be appropriate to inform them of their rights as well.

²⁴ (U) The Victim Notification System is a Department of Justice system used by the FBI, Federal Bureau of Prisons, United States Attorneys' offices, and the United States Postal Inspection Service.

into the system. Because Cyber Case A was a national security case, it was unclear whether OVA did not send letters to the victims identified in the case only because the case was a national security case, or if the victims not being indexed properly contributed to the problem.

(U) OVA informed us that it is aware of gaps in coverage for advising cybercrime victims of their rights. OVA provided three reasons for these gaps:

1. The AG Guidelines are out of date with respect to victims of cybercrime.
2. There is no widely accepted definition of what constitutes a victim of cybercrime.
3. There is currently no process for getting cybercrime victims' information from national security cases into the Victim Notification System.

(U) We discussed these issues with the Department of Justice Office of the Deputy Attorney General (ODAG). The ODAG is part of the Department of Justice's Cyber-Digital Task Force which is tasked with "canvass[ing] the many ways that the Department is combatting the global cyber threat, and...identify[ing] how federal law enforcement can more effectively accomplish its mission in this vital and evolving area." ODAG told us that it would consider updates to the AG Guidelines and a generally accepted definition of a cyber victim, and it would present these issues to the task force.

(U) While investigators are given latitude to not make notifications if it would negatively affect the investigation, we found that victims have been notified of the fact that they were victimized, but not informed of their rights under the AG Guidelines. Since the FBI determined it was operationally safe to notify the entities of their victimization, it should be appropriate to inform them of their rights as well. Due to these gaps in coverage, not all victims are being informed of their rights according to the AG Guidelines. Therefore, we recommend that the Department of Justice coordinate with the FBI's Cyber Division and update, as necessary, the Attorney General Guidelines for Victim and Witness Assistance to incorporate the nuances of cyber victims. In addition, we recommend that the FBI clearly define what constitutes a victim of cybercrime for the purposes of indexing victims in Sentinel and to ensure that all victims of cybercrime are informed of their rights under the AG Guidelines, *Crime Victims' Rights Act*, and *Victims' Rights and Restitution Act*, as appropriate.

(U) Quality and Consistency of Leads

(U) During our interviews of cyber agents at FBI field offices, agents expressed concerns about the content of leads they received requesting victim notifications. These agents said that the quality of leads varied depending on the author of the lead and less-detailed leads often made it difficult for agents who are not well versed in the details of the case to make useful notifications to victims. We believe this problem is the result of two factors. First, different field offices

conduct business in different ways, so some field offices send more detailed leads than others. Second, CyD Policy Guide 0853PG explains when victim notifications should be made, but it does not explain what information should be included in leads requesting a notification or the minimum amount of information needed to conduct a notification.

(U) We asked agents who expressed concerns about the quality and consistency of the leads they receive what information they need to be able to conduct a useful victim notification. The following is what they told us should be provided to victims in order to be helpful:

- IP addresses affected by the malicious activity,
- a date or range of dates the activity happened,
- any information about the attack that the victim can use to search for the activity in their logs, and
- an unclassified tear-line for information to share with the victim.²⁵

(U) Additionally, as discussed further in the next section of this report, we met with victims of cybercrime that told us that the quality of the information provided by the FBI at times lacked substance, making it difficult to pinpoint where the intrusion entered their system. FBI officials acknowledged issues with both the timeliness and quality of information it provides. The FBI said those issues were usually the result of classified information being involved. The intelligence the FBI receives from OGAs is almost always classified at a level of Secret or above. Agents will attempt to get as much information downgraded to the unclassified level as possible to ensure the information given to the victim is actionable. Overall, in our interviews with victims, we were told that each notification, to be useful, should include the date and time the intrusion occurred, an infected IP address, and what activity was observed.

(U) When insufficient information is shared with the victim, the victim may not be able to mitigate the threat and the relationship between the FBI and the victim—potentially a source of evidence or intelligence in the FBI’s cyber mission—can be damaged by diminishing the FBI’s credibility as a partner. The relationships between the FBI and the private sector are important sources of intelligence and evidence for ongoing investigations. Therefore, to ensure consistency and effectiveness of victim notifications, and to promote partnerships between the FBI and victims, we recommend that the FBI update Cyber Division Policy Guide

²⁵ (U) A tear-line is a section of text classified at a level lower than the rest of a document for the purpose of increased ability to share the information. For example, a classified report on a cyber-intrusion may have a secret-level tear-line to allow some of the information to be documented in Sentinel and an unclassified tear-line to allow information to be shared with a victim that does not have security clearance.

0853PG to include a minimum requirement for information that should be included in a victim notification and in victim notification leads.

(U) Victim Engagement

(U) From the Cyber Guardian data provided by the FBI, we selected and either met with or received comments from 14 victims of cybercrime that had received victim notifications from the FBI. We asked the victims to discuss their interactions with the FBI so we could learn how the notifications worked from the victim's perspective. Specifically, we discussed how the notifications took place and whether the notifications were effective from their perspective as victims. The victims we met with came from various sectors, industries, and organizations including:

- local and federal government,
- the private sector, including the technology and manufacturing sectors,
- universities, and
- public utilities.

(U) For the 14 victims we met with or received comments from, all of the victim notifications made were initiated by a phone call or an in-person meeting with an agent. According to FBI agents that we interviewed, a cyber victim notification is both a service—providing the victim with indicators of compromise and other information about the attack—and an opportunity to develop or enhance a working relationship with the victim. Relationships are vital to the FBI's cyber mission because they help the FBI gather information about cyber threats by gaining consensual access to information and networks of personnel with expertise about cyber-related topics. Victims are under no obligation to cooperate with the FBI to further the investigation of an intrusion and can deny the FBI's services. Ongoing relationships also simplify communication with victims that suffer multiple intrusions. A victim official is much more likely to take a phone call from an agent that person already knows, ultimately saving time and resources. Additionally, we were told that developed relationships also foster information sharing. Of the 14 victims with whom we discussed these interactions, 13 said they proactively share information with the FBI through the local FBI field office.

(U) Although many of the victim organizations we interviewed spoke highly of the FBI and their close relationships with their respective field offices, half of the victims we met had complaints with the timeliness and quality of the information provided. Additionally, of those 14 victims, 4 (29 percent), were not satisfied overall with their interactions, including one instance in which the FBI notified the wrong point of contact. Timely notification is critical because victims rely heavily on the information provided by the FBI to remediate the threat with as little damage to their infrastructure as possible. Because victims often keep information, such as network logs, for a limited time, the information provided to the victim needs to be recent. In one instance, a company told us it received a victim notification for an

event that took place 9 months prior. Although the information the company received from the agent was thorough, the company had issues obtaining logs that dated back 9 months and was forced to bring in a third-party remediation firm to alleviate the problems associated with the intrusion. The FBI cannot always control the amount of time that elapses between the date of a cyber-intrusion and when the intrusion is discovered, however it can control how long it takes to notify the victim once the attack and victim have been identified. Therefore, we recommend that the FBI establishes timeliness standards in the Cyber Division Policy Guide 0853PG for cyber victim notifications, as appropriate.

(U) Coordination with Other Government Agencies

(U) Cooperation and coordination with OGAs conducting notifications to victims of cybercrime is important to avoid missed or duplicative victim notifications. In order to facilitate this coordination, the agencies that comprise the other Federal Cybersecurity Centers employ the First Look Standard Operating Procedures, use Victim Contact Planning Calls, and use the Cyber Guardian System.

(U) First Look and Victim Contact Planning Call

(U) The First Look Standard Operating Procedures are maintained by both the FBI's CyWatch and DHS's NCCIC and dictate how to coordinate the U.S. government's response to newly discovered cyber incidents. This process covers activity from the initial identification of a developing cyber incident to victim notification. An agency with victim contact responsibilities, such as one of the NCIJTF partner agencies that becomes aware of a developing cyber incident, will determine whether the incident warrants a Victim Contact Planning Call (VCPC). VCPCs are interagency conference calls for coordinating initial contact with victims. If the engagement thresholds are met, the identifying agency will make a request to the Federal Cybersecurity Centers that a VCPC be scheduled. The identifying agency is responsible for facilitating and guiding the discussion during the call.

(U) The First Look Standard Operating Procedures state that initial contact of cyber victims should be coordinated if the incident poses a threat to national security or critical infrastructure, involves cyberterrorism, or has the potential to impact multiple sectors or to have cascading impacts across sectors. The FBI is responsible for all investigative matters related to the incident, while DHS is responsible for matters related to mitigation of the victim network and evaluation of the risk to critical infrastructure and key resources.

(U) According to the First Look Standard Operating procedures, VCPC participants should discuss all aspects of victim contact, including investigation and mitigation options. The objective of the VCPC discussion is to generate a coordinated plan for initial contact and subsequent engagement with the victim of a cyber-incident. All relevant information regarding the incident, including known actors, ongoing threat activity, and mitigation efforts should be shared during the

call. This information sharing is intended to ensure a comprehensive and coordinated response effort. The goal is for a VCPC to take place within 4 hours of the identification of a developing cyber-incident. If a developing cyber incident is identified outside of business hours, the goal is to conduct a VCPC within the first 4 hours of the next business day unless the nature of the incident dictates a more urgent response.

(U//FOUO) [REDACTED]

(S//NF) When we asked FBI officials why coordination only happens to a small percentage [REDACTED] of [REDACTED] incidents recorded in Cyber Guardian annually, they said that coordination only occurs on incidents labeled as "Medium" or higher on the National Security Council's Cyber Incidents Severity Schema.²⁶ [REDACTED]

[REDACTED] We found that the low number of incidents with at least a Medium severity ranking may be the result of the Severity Schema itself. We were told by the FBI that the elements of the Severity Schema are subjective, and two agents may score the same incident differently, which contributes to the small number of incidents that were classified as "Medium" during this time period.

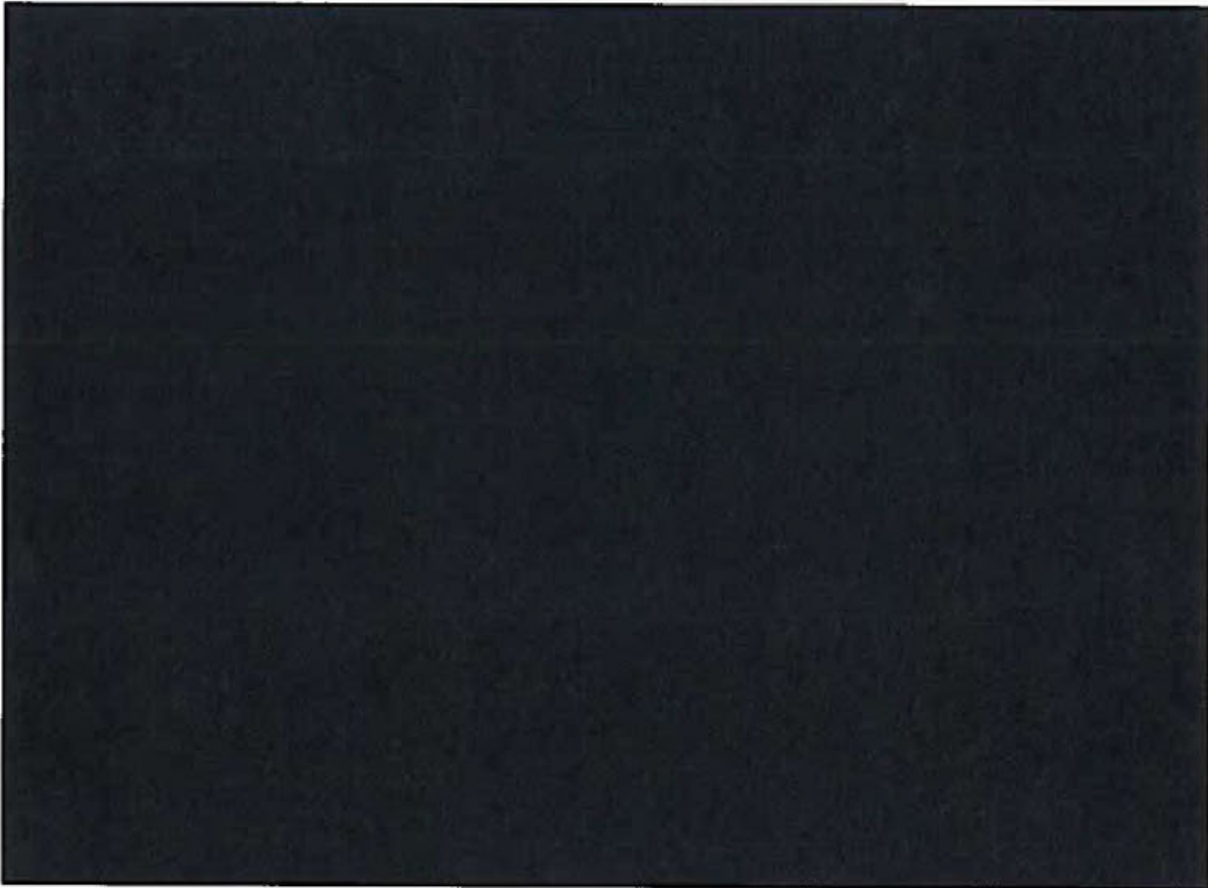
(U) We recommend that the FBI ensures Victim Contact Planning Calls are conducted for all cyber-incidents that are labeled "Medium and above" on the National Security Council's Cyber Incidents Severity Schema.

(U) Cyber Guardian Usage by Agency

(U) The FBI's partner agencies that participate in the NCIJTF have access to Cyber Guardian and the responsibility to update the system as appropriate. However, according to CyWatch, the FBI enters the bulk of data contained in Cyber Guardian. CyWatch tracks usage of Cyber Guardian by all users and provided us with the following summary of cyber incidents entered in the system by NCIJTF agencies.

²⁶ (U) Prior to the adoption of the National Security Council's Cyber Incidents Severity Schema in July 2015, the FBI used the "CyD Threat Prioritization Matrix," which required coordination on cyber incidents classified at priority level three (Elevated) or higher, which is roughly equivalent to the current severity schema.

(S//NF)



(U//FOUO)

(U) Source: FBI

(U) E.O. 13636 directs both the Departments of Justice and Homeland Security to develop and use a system to track and disseminate victim notifications, and the system created to meet this requirement is Cyber Guardian. However, according to the Cyber Guardian usage data, it appears that DHS is not entering data into the system appropriately. According to the FBI, DHS regularly conducts victim notifications, but does not enter the corresponding information into Cyber Guardian, potentially creating many notifications that are not being tracked as required by E.O. 13636.

(S//NF)

[REDACTED]

(S//NF)

[REDACTED]

(U//FOUO)

[REDACTED]

(U//FOUO)

[REDACTED]

²⁷ (U) Traffic Light Protocol includes four colors that indicate how widely the information's originator will allow the referenced information to be disseminated. Red - cannot be disseminated outside named individuals; Amber - limited within the recipient's organization to others with a need to know; Green - Community wide, not to be posted publicly; and White - unlimited distribution.

²⁸ (U) An equity evaluation is a review to determine whether disclosure of that information will negatively impact an investigation or intelligence operation.

[REDACTED]

(U) We spoke with the FBI and DHS regarding these examples and received conflicting information. While we were unable to definitively determine the root cause of the issues described in the preceding paragraphs, these examples demonstrate communication issues between the FBI and OGAs which can lead to disjointed victim notifications.

(U//FOUO) [REDACTED]

[REDACTED] Therefore, we recommend that the FBI pursue a mutually agreeable solution with DHS for ensuring all victim notification data is entered into Cyber Guardian. We also referred this matter to the DHS Office of Inspector General to take action as it deems appropriate.

(U) Challenges in Notifying Victims Identified by Other Government Agencies

(U) As stated in E.O. 13636, "It is the policy of the United States Government to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats."

(U) In addition to victims self-reporting cyber-attacks and the FBI identifying victims during the course of its investigations, OGAs will also report potential victims to the FBI. While Cyber Guardian contains data on when a cyber-threat was first observed, the victim was identified, and the victim was notified, due to the issues we found with the reliability of Cyber Guardian's data, we were unable to rely on the data in Cyber Guardian to determine the average length of time between observation of a cyber-threat and notification of the victim. Victim notifications can occur a long time after the attack for reasons beyond the controls of the notification process. For example, if an attack is not discovered immediately, a substantial time may pass between the attack and the notification. However, we also found delays in the notifications of victims identified by OGAs.

(U//FOUO) [REDACTED]

(U//FOUO) [REDACTED]

(U//FOUO) [REDACTED]

²⁹ (U) Masked U.S. identities include individuals and organization names, as well as U.S. internet protocol addresses.

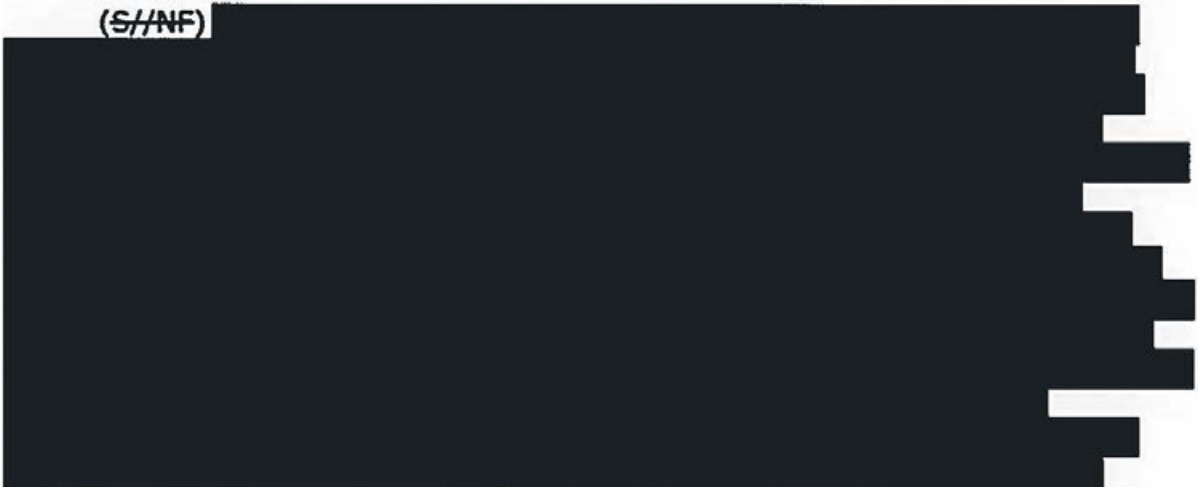
(S//NF)

A large black rectangular redaction box covering the top portion of the page content.

(U) * For FY 2018, the numbers are year to date as of January 11, 2018.

(U) Source: FBI

(S//NF)

A large black rectangular redaction box covering the middle section of the page content.

(U//FOUO)

A large black rectangular redaction box covering the bottom section of the page content.

[REDACTED] We recommend that the FBI coordinate with NSA to identify and implement an automated solution to streamline the post-publication requests for unclassified information in order to conduct timely and useful victim notifications.

(U) CyNERGY System to Replace Cyber Guardian

(U) The FBI estimated the development costs for Cyber Guardian from 2014 through 2017 were approximately \$2.2 million.³⁰ This includes the cost of a team of eight contractors responsible for software development. From 2015 through 2017, Operations and Maintenance costs were approximately \$2.5 million.³¹

(U) According to CyWatch, Cyber Guardian was intended to be an interim solution to the E.O. 13636 Section 4(b) requirement. As a result, in 2014, the NCIJTF formed a Joint Requirements Team (JRT) to determine the features needed in a new, permanent system to replace Cyber Guardian. The JRT was co-led by DHS, the Department of Justice, and the Department of Defense, and included the following agencies:

- DHS NCCIC,
- FBI,
- Defense Cyber Crime Center,
- Defense Security Service,
- NSA, and
- Other DoD Components, which included sector specific agencies and other government agencies interested in participating.

(U) The requirements proposed by the JRT were accepted by the National Security Council and memorialized in an April 10, 2015, document titled, "Executive Order (E.O.) 13636 Section 4(b) Support Capability Requirements for Notification of Critical Infrastructure Targeted Entities." The new system is named CyNERGY and the FBI's Information Technology Branch began developing CyNERGY in 2016.

(U) The costs of developing and maintaining CyNERGY are projected to be twice the costs for Cyber Guardian, and between FY 2016 and FY 2018,

³⁰ (U) The same developers supported both Guardian and Cyber Guardian and did not log their time between the two systems; therefore the FBI relied on an estimate from the vendor on the breakout of development costs between the two systems.

³¹ (U) Operations and maintenance costs for the purpose of this report include support staff for hardware, such as database and system administrators, hardware costs, and software costs such as licenses and maintenance.

development costs for CyNERGY are projected to be approximately \$4.9 million.³² Operations and maintenance costs for CyNERGY are projected to be approximately \$4.2 million during the same time period, for an average of \$1.4 million per year.

(U) In November 2017, CyWatch provided us with a demonstration of CyNERGY, which the FBI aims to deploy in FY 2019. After deployment, the FBI intends to enhance it with additional features. At initial deployment, CyNERGY will have a simplified data input, utilizing only the fields used most often in Cyber Guardian, including the:

- title of the cyber event and classification of the title,
- reporting agency and related reference number,
- receipt method,
- activity type,
- event date and time, and
- victim's information.

(U) Because CyNERGY was designed and built specifically for CyD, future changes should be much easier to make than they were with Cyber Guardian because changes will no longer need to be made by the Counterterrorism Division. CyWatch demonstrated some of CyNERGY's features that should be improvements over Cyber Guardian. One of those features queries Dun & Bradstreet's database to automatically load the Data Universal Numbering System (DUNS) number for each victim.³³ This should help lower the risk of duplicate notifications and identify previous notifications because DUNS numbers are unique and not subject to how a particular user enters a company's name into the system. According to CyWatch, another control it plans to implement will provide validity checks along with automated checks against FBI information databases to limit the manual entry of specific fields, further limiting the risk of typographical errors.

(U) CyWatch also showed us the dashboard area of the system which shows pertinent information in a more visually appealing and easy to understand format. From this view, users can easily see metrics about:

- outstanding victim notifications,
- the time between the date of attack to the event being entered in CyNERGY, and
- the time between entry in CyNERGY and notification of the victim.

³² (U) Both the development costs, and operations and maintenance costs include projections for FY 2018.

³³ (U) The DUNS number is a unique nine-character number used by Dun and Bradstreet to maintain up-to-date information on more than 285 million global businesses including information on companies' parent and sister companies.

Additionally, users from any NCIJTF agency should be able to make changes to many aspects of a cyber-event or notification, including:

- what agency is responsible for the notification,
- the severity of the event, and
- equity evaluation.

CyWatch explained that changes to an entry about an incident will be logged in an auditable way and all users who have a role in that entry will be alerted via automatic email when changes are made.³⁴

(U) As mentioned earlier, DHS has requested that a machine-to-machine application programming interface be included in CyNERGY to automatically transfer victim notification data from its internal tracking system into CyNERGY. DHS does not believe the feature will be in the initial version of the system, but it is confident the feature will be in a subsequent version. DHS expressed concerns that both the current system, Cyber Guardian, and the new system, CyNERGY, do not have controls in place to ensure that users are certified to handle Protected Critical Infrastructure Information (PCII). PCII is critical infrastructure information that is voluntarily shared with the federal government for homeland security purposes, and is protected by the Critical Infrastructure Act of 2002. We discussed this with CyWatch and it told us that the FBI ensures that new Cyber Guardian users submit proof that they have completed PCII Authorized User training on the proper handling and safeguarding of PCII before being granted access to Cyber Guardian. However, CyWatch admitted that once a user is granted access, there are no controls in place to ensure that the user takes the training annually as required to maintain authorization to handle PCII. Therefore, we recommend that the FBI implement controls to ensure that all users of Cyber Guardian, and subsequently CyNERGY, are certified to handle PCII.

(U) CyNERGY was still under development at the time of our audit so we were unable to thoroughly evaluate the system and make definitive judgments on its performance. However, based on the system requirements document and the demonstration provided by CyWatch, we believe that if implemented according to plan, there will be improvements over Cyber Guardian. While CyNERGY should address issues we identified with Cyber Guardian, we also found that some issues present in Cyber Guardian will likely remain in CyNERGY. For example, CyNERGY will rely on FBI agents using "Victim Notification" lead types for automatic ingest of FBI notifications through Sentinel. As a result, CyWatch will still need to search Sentinel for missed victim notifications to manually input into CyNERGY and, similar to the current process, this manual search will rely on agents properly indexing victims in Sentinel. In addition, CyNERGY will reside on the secret enclave and will

³⁴ (U) Roles include: notifier, mitigator, investigator, observer, and outreach.

not solve the issue with DHS having difficulty entering information into Cyber Guardian. These problems may result in manual errors; therefore, we recommend that the FBI ensures that CyNERGY's data input is as automated as appropriate.

(U) CONCLUSION AND RECOMMENDATIONS

(U) We found that in response to Executive Order 13636, Improving Critical Infrastructure Cybersecurity, Section 4(b), the FBI, in conjunction with partner agencies, developed and deployed Cyber Guardian, a system to track and disseminate notifications to victims of cybercrime. Although FBI and DHS personnel agree that the coordination of victim notifications has improved significantly since E.O. 13636 was signed and while Cyber Guardian has been a useful tool for this purpose, we found issues with the completeness and the quality of the data stored in the system. The system relies too heavily on manual input of data that leads to errors and poor data reliability.

(U) We also found that FBI cyber agents are not following procedures for setting victim notification leads or indexing victims properly, resulting in some notifications not being tracked in Cyber Guardian as required. The FBI also needs to ensure that notifications made to victims identified in restricted access cases are properly tracked in Cyber Guardian. The CyD Policy Guide 0853PG details when notifications should be made to victims of cybercrime, which can help victims mitigate the damage caused by current and future intrusions and increase the potential for intelligence collection by the FBI, but does not describe how to conduct those notifications. We found that this has led to inconsistency in the quality of leads sent between field offices which, in turn, negatively affects the quality and timeliness of notifications made to victims of cybercrime. Half of the victims we met with complained that they have received at least one notification too late or without enough detail to allow the victims to mitigate the threats to their systems, although sometimes this is due to factors outside the FBI's control. Despite DHS being identified as a partner to the FBI in E.O. 13636, we found that DHS is not entering data into Cyber Guardian as required. The FBI is developing a new system called CyNERGY to replace Cyber Guardian and, although we were unable to test the system, we believe that if CyNERGY operates as intended, it could provide improvements to the current system. However, CyNERGY will still rely on manual data entry. Finally, victims of cybercrimes investigated in national security cases are not being notified of their rights in accordance with the Attorney General Guidelines for Victim and Witness Assistance.

(U) We recommend that the FBI:

1. (U) Ensure there are appropriate logic controls for data that is manually input into Cyber Guardian and CyNERGY, and that CyNERGY's data input is as automated as appropriate.
2. (U) Strengthen controls for ensuring that victim notifications are tracked in Cyber Guardian, to include agents using "Victim Notification" leads in Sentinel as required by Cyber Division Policy Guide 0853PG.

3. (U) Ensure that agents index "Victims" in Sentinel as required by the Indexing User Manual for Sentinel to support FBI investigative and administrative matters.
4. (U) Ensure that all cyber victim notifications conducted in the course of restricted investigations are appropriately tracked in Cyber Guardian.
5. (U) Clearly define what constitutes a victim of cybercrime for the purposes of indexing victims in Sentinel and notifying victims of their rights under the Attorney General Guidelines for Victim and Witness Assistance, as appropriate.
6. (U) Ensure that all victims of cybercrime are informed of their rights under the Attorney General Guidelines for Victim and Witness Assistance, Crime Victims' Rights Act, and Victims' Rights and Restitution Act, as appropriate.
7. (U) Establish timeliness standards in the Cyber Division Policy Guide 0853PG for cyber victim notifications, as appropriate.
8. (U) Update Cyber Division Policy Guide 0853PG to include a minimum requirement for information that should be included in a victim notification and in victim notification leads, to ensure the consistency and effectiveness of victim notifications.
9. (U) Ensure Victim Contact Planning Calls are conducted for all cyber-incidents that are labeled "Medium and above" on the National Security Council's Cyber Incidents Severity Schema.
10. (U) Pursue a mutually agreeable solution with DHS for ensuring all victim notification data is entered into Cyber Guardian.
11. (U) Coordinate with NSA to identify and implement an automated solution to streamline the post-publication requests for unclassified information in order to conduct timely and useful victim notifications.
12. (U) Implement controls to ensure that all users of Cyber Guardian, and subsequently CyNERGY, are certified to handle Protected Critical Infrastructure Information.

(U) We recommend that the Department of Justice:

13. (U) Coordinate with the FBI's Cyber Division and update, as necessary, the Attorney General Guidelines for Victim and Witness Assistance to incorporate the nuances of cyber victims.

(U) STATEMENT ON INTERNAL CONTROLS

(U) As required by the *Government Auditing Standards*, we tested, as appropriate, internal controls significant within the context of our audit objective. A deficiency in an internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to timely prevent or detect: (1) impairments to the effectiveness and efficiency of operations, (2) misstatements in financial or performance information, or (3) violations of laws and regulations. Our evaluation of the FBI's internal controls was not made for the purpose of providing assurance on its internal control structure as a whole. FBI management is responsible for the establishment and maintenance of internal controls.

(U) As noted in the Audit Results section of this report, we identified deficiencies in the FBI's internal controls that are significant within the context of the audit objective and based upon the audit work performed that we believe may adversely affect the FBI's ability to effectively track and disseminate notifications to all identified victims of cybercrime.

(U) Because we are not expressing an opinion on the FBI's internal control structure as a whole, this statement is intended solely for the information and use of the FBI. This restriction is not intended to limit the distribution of this report, which is a matter of public record. However, we are limiting the distribution of this report because it contains sensitive information that must be appropriately controlled.³⁵

³⁵ (U) A redacted copy of this report with sensitive information removed will be made available publicly.

(U) STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS

(U) As required by the *Government Auditing Standards*, we tested, as appropriate given our audit scope and objective, selected transactions, records, procedures, and practices to obtain reasonable assurance that the FBI's management complied with federal laws and regulations for which noncompliance, in our judgment, could have a material effect on the results of our audit. FBI's management is responsible for ensuring compliance with applicable federal laws and regulations. In planning our audit, we identified the following laws and regulations that concerned the operations of the auditee and that were significant within the context of the audit objective:

- Executive Order 13636
- Presidential Policy Directive-41
- Attorney General Guidelines for Victim and Witness Assistance

(U) Our audit included examining, on a test basis, the FBI's compliance with the aforementioned laws and regulations that could have a material effect on the FBI's operations, through interviewing FBI personnel, analyzing data, examining procedural practices, and assessing internal control procedures. As noted in the Audit Results section of this report, we found that the FBI did not comply with the Attorney General Guidelines for Victim and Witness Assistance.

(U) APPENDIX 1

(U) OBJECTIVE, SCOPE, AND METHODOLOGY

(U) Objective

(U) The objective of our audit was to evaluate the FBI's Cyber Victim Notification and Engagement Process.

(U) Scope and Methodology

(U) We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

(U) To accomplish our objective, we interviewed 51 FBI officials, including individuals from the FBI's CyWatch unit and other components that are involved in the cyber victim notification process, Cyber Division Headquarters and the Office of Victim Assistance. We visited 6 FBI field offices, including Washington, Boston, New Haven, Philadelphia, Chicago, and Baltimore. We also interviewed staff from the National Security Agency's National Cyber Threat Operations Center and the Department of Homeland Security's National Cybersecurity and Communications Integration Center to learn about their interaction with the FBI's cyber victim notification process. In addition, we met with, or received comments from, 14 organizations that received victim notifications from the FBI to discuss those interactions. The scope of our audit generally covered cyber victim notification activity from November 2014 to December 2017 (approximately 20,000 Cyber Guardian entries).

(U) We reviewed Cyber Division policy, guidance, plans and assessments including FBI Cyber Division Policy Guide 0853PG, Dated February 14, 2017, Executive Order 13636, Improving Critical Infrastructure Cybersecurity, and Presidential Policy Directive 41 "United States Cyber Incident Coordination." To assess victim notification internal controls, we reviewed the Attorney General Guidelines for Victim and Witness Assistance, along with the two laws that support those guidelines, the *Victims' Rights and Restitution Act of 2006*, and the *Crime Victims' Rights Act of 2006* (supplemented in 2009).

(U) APPENDIX 2

(U) FEDERAL BUREAU OF INVESTIGATION'S RESPONSE TO
THE DRAFT AUDIT REPORT



U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

December 21, 2018

(U) The Honorable Michael E. Horowitz
Inspector General
Office of the Inspector General
U.S. Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, DC 20530

(U) Dear Mr. Horowitz:

(U) The Federal Bureau of Investigation (FBI) appreciates the opportunity to review and respond to your office's report entitled, *Audit of the Federal Bureau of Investigation's Cyber Victim Notification Process*.

(U) We agree that it is important to strengthen procedures for setting victim notification leads and indexing victims. Additionally, we agree it is imperative that victims of cybercrime are informed of their rights under the requisite authorities. In that regard, we concur with your twelve recommendations for the FBI.

(U) Should you have any questions, feel free to contact me. We greatly appreciate the professionalism of your audit staff throughout this matter.

(U) Sincerely,

A handwritten signature in blue ink, appearing to read "Suzanne Turner", is positioned above the typed name.

(U) Suzanne Turner
Section Chief
External Audit and Compliance Section
Inspection Division

(U) Enclosure

(U) The Federal Bureau of Investigation's (FBI) Response to the Office of the Inspector General's Audit of the FBI's Cyber Victim Notification Process

- (U) **Recommendation #1:** "The OIG recommends the FBI ensure there are appropriate logic controls for data that is manually input into Cyber Guardian and CyNERGY, and that CyNERGY's data input is as automated as appropriate."
- (U) **FBI Response to Recommendation #1:** Concur. Working through the Sentinel team, FBI will develop structured fields (e.g., pick lists, validated form fields, mandatory fields) within the victim data cards in order to ensure complete and accurate data entry and enable automated pulling of data from Sentinel to Cyber Guardian/Cynergy.
- (U) **Recommendation #2:** "The OIG recommends the FBI strengthen controls to ensure victim notifications are tracked in Cyber Guardian, to include agents using "Victim Notification" leads in Sentinel as required by Cyber Division Policy Guide 0853PG."
- (U) **FBI Response to Recommendation #2:** Concur. Working through the Sentinel team, Cyber Division will work to update the technical process to allow for the automated ingest of data. Cyber Division will update its policy guide to reflect the requirement to report victim notifications (e.g. "should report" to "will report") to CyWatch for inclusion in Cyber Guardian. Additionally, Cyber Division will execute training and an awareness campaign for the use of victim notification leads.
- (U) **Recommendation #3:** "The OIG recommends the FBI ensure agents index "Victims" in Sentinel as required by the Indexing User Manual for Sentinel to support FBI investigative and administrative matters."
- (U) **FBI Response to Recommendation #3:** Concur. Cyber Division will execute training and an awareness campaign for the use of indexing, per policy.
- (U) **Recommendation #4:** "The OIG recommends the FBI ensure that all victim notifications conducted in the course of restricted investigations are appropriately tracked in Cyber Guardian."
- (U) **FBI Response to Recommendation #4:** Concur. Cyber Division conducts sensitive investigations that require restricted designations. In these instances, Cyber Division will comply with victim notification policy with regards to the actual victim. However, victim notification reporting for inclusion in Cyber Guardian may be delayed as CyWatch does not have visibility into restricted cases.
- (U) **Recommendation #5:** "The OIG recommends the FBI clearly define what constitutes a victim of cybercrime for the purposes of indexing victims in Sentinel and notifying victims of their rights under the Attorney General Guidelines for Victim Witness Assistance, as appropriate."

- (U)**FBI Response to Recommendation #5:** Concur. Cyber Division will work with OGC's National Security and Cyber Law Branch (NSCLB) to ensure there is clear guidance and a definition for what or whom constitutes a victim of cybercrime for purposes of Sentinel indexing. Cyber Division will also work closely with OGC's NSCLB to get guidance, as needed, with regard to the Attorney General Guidelines for Victim Witness Assistance in order to ensure the Guidelines are being followed, when appropriate.
- (U)**Recommendation #6:** "The OIG recommends the FBI ensure that all victims of cybercrime are informed of their rights under the Attorney General Guidelines for Victim and Witness Assistance, Crime Victims' Rights Act, and Victims' Rights and Restitution Act, as appropriate."
- (U)**FBI Response to Recommendation #6:** Concur. Within six months of the completion of the report, VSD will work with CyD to ensure that notice to victims of cybercrime, whether the notice comes from CyD or from VSD, includes basic information on their rights under the Attorney General Guidelines for Victim and Witness Assistance, Crime Victims' Rights Act, and Victims' rights and Restitution Act, as appropriate, as well as a VSD point of contact for accessing their rights and any appropriate and available victim assistance services. VSD will also participate in any efforts coordinated by DOJ to update the Attorney General Guidelines for Victim and Witness Assistance (2011) to incorporate guidance on cybercrime victim notification and assistance.
- (U)**Recommendation #7:** "The OIG recommends the FBI establish timeliness standards in the Cyber Division Policy Guide 0853PG for cyber victim notification, as appropriate."
- (U)**FBI Response to Recommendation #7:** Concur. Cyber Division will incorporate additional guidance regarding timeliness of victim notification into its policy guide.
- (U)**Recommendation #8:** "The OIG recommends the FBI update Cyber Division Policy Guide 0853PG to include a minimum requirement for information that should be included in a victim notification and in victim notification leads, to ensure the consistency and effectiveness of victim notification."
- (U)**FBI Response to Recommendation #8:** Concur. Cyber Division will update its policy guide to reflect minimum requirements as outlined in the recommendation.
- (U)**Recommendation #9:** "The OIG recommends the FBI ensure Victim Contact Planning Calls are conducted for all cyber incidents that are labeled "Medium and above" on the National Security Council's Cyber Incidents Severity Schema."
- (U)**FBI Response to Recommendation #9:** Concur. CyWatch will initiate Victim Contact Planning Calls (VCPCs), as recommended, and make corresponding changes to its watch procedures.

- (U)**Recommendation #10:** “The OIG recommends the FBI pursue a mutually agreeable solution with DHS for ensuring all victim notification data is entered into Cyber Guardian.”
- (U)**FBI Response to Recommendation #10:** Concur. Cyber Division will pursue a solution with DHS executive management regarding Cyber Guardian/Cynergy data submission.
- (U)**Recommendation #11:** “The OIG recommends the FBI coordinate with NSA to identify and implement an automated solution to streamline the post-publication requests for unclassified information in order to conduct timely and useful victim notifications.”
- (U)**FBI Response to Recommendation #11:** Concur. Cyber Division will coordinate with NSA to identify and implement solutions to streamline post-publication requests, which may include automated solutions and new dissemination policies.
- (U)**Recommendation #12:** “The OIG recommends the FBI implement controls to ensure that all users of Cyber Guardian, and subsequently CyNERGY, are certified to handle Protected Critical Infrastructure Information.”
- (U)**FBI Response to Recommendation #12:** Concur. Cyber Guardian currently has the capability for incident and note restrictions, allowing users to restrict information such as PII or PCII. Cynergy will also have a similar feature to restrict information at the first release to production. One of the future requirement enhancements to Cynergy is to have a features in user’s profile to restrict a user from viewing PII or PCII information until training has been completed and a certificate has been provided.

(U) APPENDIX 3

**(U) OFFICE OF THE DEPUTY ATTORNEY GENERAL'S
RESPONSE TO THE DRAFT AUDIT REPORT**



U.S. Department of Justice

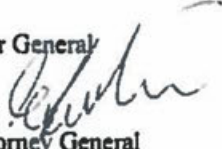
Office of the Deputy Attorney General

Associate Deputy Attorney General

Washington, D.C. 20530

(U) MEMORANDUM

(U) TO: Michael Horowitz
Inspector General
Office of the Inspector General

(U) FROM: Bradley Weinsheimer 
Associate Deputy Attorney General
Office of the Deputy Attorney General

(U) DATE: February 19, 2019

(U) SUBJECT: Department of Justice Comments on Draft Audit Report – Audit of The Federal Bureau of Investigation's Cyber Victim Notification Process

(U) Thank you for the opportunity to comment on your draft audit report, "Audit of The Federal Bureau of Investigation's Cyber Victim Notification Process." In the draft report, you have made the following recommendation (Recommendation 13) to the Department of Justice (Department): We recommend that the Department of Justice coordinate with the FBI's Cyber Division and update, as necessary, the Attorney General Guidelines for Victim and Witness Assistance to incorporate the nuances of cyber victims.

(U) As you know, for a number of reasons, the Department objected to the language of the recommendation as imprecise and unclear. To the extent the recommendation is intended to recommend that the Department of Justice consider updating the Attorney General Guidelines for Victim and Witness Assistance (Guidelines) to incorporate the nuances of identifying cyber victims, the Department does not oppose the recommendation. Indeed, as you know, the Department, including the FBI's Cyber Division, is actively engaged in reviewing and proposing updates as appropriate to the Guidelines on victim and witness notification.

(U) APPENDIX 4

(U) OFFICE OF THE INSPECTOR GENERAL ANALYSIS AND SUMMARY OF ACTIONS NECESSARY TO CLOSE THE REPORT

(U) The OIG provided a draft of this audit report to the Federal Bureau of Investigation (FBI) and the Office of the Deputy Attorney General (ODAG). The FBI's response is incorporated in Appendix 2 of this final report and ODAG's response is in Appendix 3. In response to our audit report, the FBI concurred with our recommendations and discussed the actions it will implement in response to our findings. The ODAG did not oppose our recommendation. As a result, the status of the audit report is resolved. The following provides the OIG analysis of the responses and summary of actions necessary to close the report.

(U) Recommendations for the FBI:

- 1. (U) Ensure there are appropriate logic controls for data that is manually input into Cyber Guardian and CyNERGY, and that CyNERGY's data input is as automated as appropriate.**

(U) Resolved. The FBI concurred with our recommendation. In its response, the FBI stated that it is working to develop structured fields within Sentinel to ensure complete and accurate data entry and enable automated pulling of data from Sentinel to Cyber Guardian and CyNERGY.

(U) This recommendation can be closed when we receive evidence that the FBI has implemented appropriate logic controls for data manually entered into Cyber Guardian and CyNERGY and that CyNERGY's data input is automated as appropriate.

- 2. (U) Strengthen controls for ensuring victim notifications are tracked in Cyber Guardian, to include agents using "Victim Notification" leads in Sentinel as required by Cyber Division Policy Guide 0853PG.**

(U) Resolved. The FBI concurred with our recommendation. In its response, the FBI stated that the Cyber Division will work to update the technical process to allow for the automated ingest of data. In addition, Cyber Division will execute training and an awareness campaign for the use of victim notification leads.

(U) This recommendation can be closed when we receive evidence that the FBI has ensured victim notifications are tracked in Cyber Guardian, including agents using "Victim Notification" leads in Sentinel as required by Cyber Division Policy Guide 0853PG.

3. **(U) Ensure that agents index "Victims" in Sentinel as required by the Indexing User Manual for Sentinel to support FBI investigative and administrative matters.**

(U) Resolved. The FBI concurred with our recommendation. In its response, the FBI stated that the Cyber Division will execute training and an awareness campaign for the use of indexing.

(U) This recommendation can be closed when we receive evidence that the FBI has ensured that agents index "Victims" in Sentinel as required by the Indexing User Manual for Sentinel to support FBI investigative and administrative matters.

4. **(U) Ensure that all cyber victim notifications conducted in the course of restricted investigations are appropriately tracked in Cyber Guardian.**

(U) Resolved. The FBI concurred with our recommendation. However, in its response, the FBI stated that it will comply with victim notification policy to notify victims identified in restricted cases, but including those notifications in Cyber Guardian may be delayed because CyWatch does not have visibility into restricted cases.

(U) This recommendation can be closed when we receive evidence that victim notifications conducted in restricted investigations are documented in Cyber Guardian.

5. **(U) Clearly define what constitutes a victim of cybercrime for the purposes of indexing victims in Sentinel and notifying victims of their rights under the Attorney General Guidelines for Victim and Witness Assistance, as appropriate.**

(U) Resolved. The FBI concurred with our recommendation. In its response, the FBI stated that the Cyber Division will work with the FBI Office of General Counsel's National Security and Cyber Law Branch to ensure there is clear guidance and definition of what or whom constitutes a victim of cybercrime for the purpose of indexing in Sentinel. The Cyber Division will also work with the National Security and Cyber Law Branch to ensure victims are notified of their rights under the Attorney General Guidelines when appropriate.

(U) This recommendation can be closed when we receive evidence that the FBI has clearly defined what constitutes a victim of cybercrime for the purposes of indexing victims in Sentinel and is notifying victims of their rights under the Attorney General Guidelines for Victim and Witness Assistance, as appropriate.

6. **(U) Ensure that all victims of cybercrime are informed of their rights under the Attorney General Guidelines for Victim and Witness Assistance, Crime Victims' Rights Act, and Victims' Rights and Restitution Act, as appropriate.**

(U) Resolved. The FBI concurred with our recommendation. In its response, the FBI stated that within six months of the issuance of this report, the Victim Services Division will work with the Cyber Division to ensure that cybercrime victim notifications include basic information on their rights under the Attorney General Guidelines for Victim and Witness Assistance, Crime Victims' Rights Act, and Victims' Rights and Restitution Act, as appropriate. The FBI will also provide the victim with a point of contact at Victim Services Division to help the victim access any available services. Finally, the FBI stated that the Victim Services Division will participate in any Department of Justice efforts to update the Attorney General Guidelines to incorporate guidance on cybercrime victim notification and assistance.

(U) This recommendation can be closed when we receive evidence that victim notifications include information about the victims' rights under the Attorney General Guidelines for Victim and Witness Assistance, Crime Victims' Rights Act, and Victims' Rights and Restitution Act, as appropriate.

7. **(U) Establish timeliness standards in the Cyber Division Policy Guide 0853PG for cyber victim notifications, as appropriate.**

(U) Resolved. The FBI concurred with our recommendation. In its response, the FBI stated that the Cyber Division will incorporate additional guidance regarding timeliness of victim notification into its policy guide.

(U) This recommendation can be closed when we receive evidence that the FBI has updated the Cyber Division Policy Guide to include timeliness standards.

8. **(U) Update Cyber Division Policy Guide 0853PG to include a minimum requirement for information that should be included in a victim notification and in victim notification leads, to ensure the consistency and effectiveness of victim notifications.**

(U) Resolved. The FBI concurred with our recommendation. In its response, the FBI stated that the Cyber Division will update its policy guide to include minimum standards for information include in victim notifications.

(U) This recommendation can be closed when we receive evidence that the FBI has updated the Cyber Division Policy Guide to include a minimum requirement for information that should be included in a victim notification and in victim notification leads.

9. **(U) Ensure Victim Contact Planning Calls are conducted for all cyber-incidents that are labeled "Medium and above" on the National Security Council's Cyber Incidents Severity Schema.**

(U) Resolved. The FBI concurred with our recommendation. In its response, the FBI stated that it will make the Victim Contact Planning Calls as recommended and update its procedures accordingly.

(U) This recommendation can be closed when we receive evidence that the FBI has ensured Victim Contact Planning Calls are conducted for all cyber-incidents that are labeled "Medium and above" on the National Security Council's Cyber Incidents Severity Schema.

10. **(U) Pursue a mutually agreeable solution with DHS for ensuring all victim notification data is entered into Cyber Guardian.**

(U) Resolved. The FBI concurred with our recommendation. In its response, the FBI stated that the Cyber Division will pursue a solution with the Department of Homeland Security's (DHS) executive management regarding entering data into Cyber Guardian and Cynergy.

(U) This recommendation can be closed when we receive evidence that the FBI has pursued a mutually agreeable solution with DHS for ensuring all victim notification data is entered into Cyber Guardian and Cynergy.

11. **(U) Coordinate with NSA to identify and implement an automated solution to streamline the post-publication requests for unclassified information in order to conduct timely and useful victim notifications.**

(U) Resolved. The FBI concurred with our recommendation. In its response, the FBI stated that it will coordinate with NSA determine a way to streamline the post-publication process for unclassified victim notification information.

(U) This recommendation can be closed when we receive evidence that the FBI has coordinated with NSA to streamline the process for receiving unclassified NSA information in order to conduct timely and useful victim notifications.

12. **(U) Implement controls to ensure that all users of Cyber Guardian, and subsequently CyNERGY, are certified to handle Protected Critical Infrastructure Information.**

(U) Resolved. The FBI concurred with our recommendation. In its response, the FBI stated that Cyber Guardian already has the capability to restrict

Protected Critical Infrastructure Information. In addition to that capability, the FBI also said that CyNERGY will have future feature that will restrict a user from viewing Protected Critical Infrastructure Information until training has been completed and a certificate has been provided.

(U) This recommendation can be closed when we receive evidence that the FBI has implemented controls to ensure that all users of Cyber Guardian, and subsequently CyNERGY, are certified to handle Protected Critical Infrastructure Information.

(U) Recommendation for the Department of Justice:

13. **(U) Coordinate with the FBI's Cyber Division and update, as necessary, the Attorney General Guidelines for Victim and Witness Assistance to incorporate the nuances of cyber victims.**

(U) Resolved. The Office of the Deputy Attorney General objected to the language of the recommendation, but did not oppose the intent of the recommendation. According to the ODAG, the Department and the FBI Cyber Division is actively engaged in reviewing and proposing updates, as appropriate to the Attorney General Guidelines for Victim and Witness Assistance.

(U) This recommendation can be closed when we receive evidence that the ODAG and FBI Cyber Division have reviewed the Attorney General Guidelines for Victim and Witness Assistance and determined whether updates are necessary to incorporate the nuances of cyber victims.



The Department of Justice Office of the Inspector General (DOJ OIG) is a statutorily created independent entity whose mission is to detect and deter waste, fraud, abuse, and misconduct in the Department of Justice, and to promote economy and efficiency in the Department's operations.

To report allegations of waste, fraud, abuse, or misconduct regarding DOJ programs, employees, contractors, grants, or contracts please visit or call the **DOJ OIG Hotline** at oig.justice.gov/hotline or (800) 869-4499.

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

950 Pennsylvania Avenue, Northwest
Suite 4706
Washington, DC 20530-0001

Website	Twitter	YouTube
oig.justice.gov	@JusticeOIG	JusticeOIG

Also at [Oversight.gov](https://www.oversight.gov)