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

Audit of the Federal Bureau of Investigation's Cyber Threat Prioritization

Audit Division 16-20 July 2016

REDACTED – FOR PUBLIC RELEASE

AUDIT OF THE FEDERAL BUREAU OF INVESTIGATION'S CYBER THREAT PRIORITIZATION

EXECUTIVE SUMMARY*

The Federal Bureau of Investigation (FBI) investigates domestic cyber attacks by criminals, overseas adversaries, and terrorists. In October 2015, FBI Director James B. Comey, Jr. testified that the FBI continues to see an increase in the scale of cyber activity as measured by the amount of data stolen or deleted and cited the Office of Personnel Management intrusion as one prominent example.[1] Protecting the United States against cyber-based attacks and high-technology crimes is the FBI's number three priority, behind counterterrorism and counterintelligence. Additionally, according to the FBI, computer intrusions involving national security are the FBI Cyber Division's highest investigative priority.

Once a year, the FBI goes through a process to establish its most severe and substantial threats.[2] This process, known as Threat Review and Prioritization (TRP), intends to direct the allocation of resources to address the highest rated threats. For this audit, we examined how the FBI prioritized cyber threats from FY 2014 through FY 2016. While we view the FBI's efforts to prioritize threats across the enterprise as a vital step in the mitigation process, we believe that TRP's subjective terminology is a substantial weakness in the FBI's efforts at prioritizing cyber threats. Because the criteria used in the TRP process are subjective and open to interpretation, we determined that the FBI's TRP process does not prioritize cyber threats in an objective, data-driven, reproducible, and auditable manner. We believe that the Cyber Division's threat prioritization process should use an algorithmic, objective, and data-driven methodology; and should produce auditable rankings. Furthermore, we believe that because the TRP is a subjective process, cyber threats that require the greatest resources may not receive the highest priority. In addition, because TRP is conducted annually, we found that TRP may not be agile enough to identify emerging cyber threats in a timely manner.

---

* The full version of this report contains classified and other information that if released publicly could compromise national security interests and the Federal Bureau of Investigation's operations. To create this public version of the report, the Office of the Inspector General redacted (blacked out) portions of the full report.

[1] James B. Comey, Jr., Director, Federal Bureau of Investigation, before the Homeland Security Committee, U.S. House of Representatives, concerning 'Worldwide Threats and Homeland Security Challenges', (October 21, 2015), https://www.fbi.gov/news/testimony/worldwide-threats-and-homeland-security-challenges (accessed March 11, 2016).

[2] In this report we use the term "threat" and we intend it to be synonymous with "threat set" and "threat issue." The FBI Cyber Division uses the term "threat set" to refer to a specific threat actor intrusion, which may be comprised of one or more actors but associated as one. Enterprise-wide, the FBI Threat Review and Prioritization process uses the term "threat issue" or "threat" to refer to a specific threat topic within a subprogram identified with an actor type and activity type or vulnerability.

However, we also found that the FBI Cyber Division has made progress in developing and utilizing a data-driven, objective methodology to augment the TRP process. That model, named the Threat Examination and Scoping (TExAS) tool, uses a weighted algorithm to prioritize cyber threats based on specific data, rather than on subjective determinations as used in the TRP process.

Further implementation of TExAS has been hampered by the lack of written policies and procedures outlining who should enter the data and how the data should be used to inform the Cyber Division's TRP process. While the Cyber Division has not developed written policies and procedures outlining who should enter the data and how the data should be used in conjunction with TRP, we found the data driven requirement of TExAS to be beneficial in the prioritization of threats. We also found that entering data into TExAS is time consuming because it is not integrated with Sentinel, the FBI's case management system. If the FBI achieves the intended integration with Sentinel, TExAS can be updated more frequently than once a year. With more frequently refreshed data, we believe that TExAS, or a system of similar ability, has the potential to provide a current picture of the cyber threat landscape, including emerging cyber threats as well as known threats that are adapting techniques, tactics, and procedures that receive little emphasis in the annual FBI TRP process. While we believe that the development of the TExAS tool is not fully mature and the results it produces are only as good as the data entered into it, we believe the use of the TExAS tool represents a best practice that could streamline and improve the prioritization within the Cyber Division, and potentially across other FBI programmatic areas as well.

As a related matter, we found, and the FBI acknowledged, that it is not currently possible to track the resources allocated to each cyber threat because the FBI's existing Time Utilization and Record Keeping (TURK) system tracks resource utilization by case classification, but not by threat. Because the FBI cannot track resources dedicated to each threat, it cannot ensure that resources are being applied to threats appropriately. Additionally, without the ability to track the time agents spend by threat, the FBI cannot be sure that it is aligning its cyber resources to its highest priority threats, a vital capability for a threat-driven organization in the current cyber climate.

This report contains two recommendations to assist the FBI in cyber threat prioritization and cyber resource allocation to address this significant and growing threat to our national security.

AUDIT OF THE FEDERAL BUREAU OF INVESTIGATION'S CYBER THREAT PRIORITIZATION

TABLE OF CONTENTS

AUDIT OF THE FEDERAL BUREAU OF INVESTIGATION'S CYBER THREAT PRIORITIZATION

INTRODUCTION

The Federal Bureau of Investigation (FBI) investigates domestic cyber attacks by criminals, overseas adversaries, and terrorists. The FBI Director recently testified that the FBI continues to see an increase in the scale of cyber activity that can be measured by the amount of data stolen or deleted and cited the Office of Personnel Management intrusion as one prominent example.[3] Protecting the United States against cyber-based attacks and high-technology crimes is the FBI's number three priority, behind counterterrorism and counterintelligence.

The FBI has found that the range of actors conducting cyber-based attacks include spies from nation-states who seek secrets and intellectual property; organized criminals who want to steal personal identities and money; terrorists intent on attacking the power grid, water supply, or other infrastructure; and "hacktivists" who are politically motivated to make a statement through their conduct. The FBI investigates all of these types of attacks to determine the actors responsible for the intrusions.

Background

The strategic objective of the FBI's Cyber Division is to proactively identify, pursue, and defeat cyber threat perpetrators while protecting the freedom, privacy, and civil liberties of U.S. persons. In October 2012, as part of its Next Generation Cyber Initiative, the FBI's Cyber Division was restructured to focus solely on computer intrusions, including combating cyber-based terrorism, hostile foreign intelligence operations conducted over the internet, and criminal computer intrusions.[4] The FBI transferred responsibility for the investigation of crimes not focused on intrusions, such as child pornography and internet money laundering, from the Cyber Division to the Criminal Investigative Division. This shift was intended to allow the FBI Cyber Division to sharpen its focus on intrusions into government and private computer networks.

According to the FBI, computer intrusion matters involving national security are the highest priority matters investigated by the FBI Cyber Division. National security computer intrusion matters are intrusions or attempted intrusions into any computer or information system that may compromise the confidentiality, integrity,

---

[3] James B. Comey, Jr., Director, Federal Bureau of Investigation, before the Homeland Security Committee, U.S. House of Representatives, concerning 'Worldwide Threats and Homeland Security Challenges', (October 21, 2015), https://www.fbi.gov/news/testimony/worldwide-threats-and-homeland-security-challenges (accessed March 11, 2016).

[4] See U.S. Department of Justice Office of the Inspector General, Audit of the Federal Bureau of Investigation's Implementation of its Next Generation Cyber Initiative, Audit Report 15-29 (July 2015).

or availability of critical infrastructure data, components, or systems (e.g., cyber national security incidents or threats to the national information infrastructure) by or on behalf of a foreign power, or an agent of a foreign power, to include designated international terrorist groups. [redacted]

In FY 2015, to ensure that the highest ranked threats are efficiently investigated, the Cyber Division implemented its Cyber Threat Team (CTT) model. A CTT focuses on the investigation of and operations against a specific national security threat. Each CTT is comprised of lead field office, called a Strategic Threat Execution office, up to five field offices assisting in specific aspects of the threat called Tactical Threat Execution offices, and a Cyber Division headquarters threat manager. The CTT bears the responsibility for managing the strategy, operations, and intelligence for its assigned threat. [redacted]

The intention of the Cyber Division's CTT model is to facilitate the allocation of resources to cyber national security threats, increase efficiency in addressing those threats, and facilitate the development of subject matter expertise within various field offices. Additionally, the CTT model is intended to enable each field office to focus on specific, assigned threats, helping to prevent the previous diffusion of efforts wherein multiple field offices were working the same cyber threat and not coordinating efforts. Prior to the implementation of the CTT, such overlapping investigations were a great challenge for the FBI. While its field offices each have a territory for which they are responsible, cyber threats are not restricted by geographical boundaries, so a territorial model proved ineffective. Lastly, the CTT model is intended to assist the FBI in prioritizing and properly allocating resources to each field office based on the threats on which they are assigned to work.

The Cyber Division organizes its headquarters national security intrusion threat operational units geographically, including sections responsible for identifying, pursuing, and defeating cyber adversaries emanating from Asia,

---

[5] A threat set is a specific threat actor group which may be comprised of one or more actors but associated as one.

[6] NTPs represent those threat issues that carry the highest potential for both significant damage to national security interests or public safety and the highest need for additional investigative and intelligence efforts to be effectively addressed. The operational division Assistant Director approves this division-level prioritization; however, final approval of all banded threats – including NTPs – rests with the FBI Deputy Director.

Eurasia, and Middle East/Africa. Such geographic delineations of responsibility do not present the same problems at Cyber Division Headquarters, since responsibility for the threats is based on their point or area of origin, and not the multiple U.S. jurisdictions where they might have an impact. The threat operational units coordinate with the CTTs and with units of the Cyber Intelligence Section, which also are geographically organized and provide actionable intelligence information.[7]

To support the Cyber Division mission, the FBI receives its funding in two ways. The FBI receives direct funding through fiscal year appropriations as part of the Department of Justice budget. In FY 2016, the FBI Cyber Division received $75.3 million in direct funding. In addition, the FBI receives funding through the National Intelligence Program (NIP). The NIP provides funding to six federal departments including the FBI, as well as the Central Intelligence Agency, and the Office of the Director of National Intelligence. The NIP funds the United States Intelligence Community activities such as intelligence collection, analysis, and the dissemination of that intelligence to inform decision making. [redacted]

[7] The Cyber Intelligence Section is comprised of the following units: Cyberterrorism Intelligence Unit, Cyber Intelligence Program Unit, Asia Cyber Intelligence Unit, Eurasia Cyber Intelligence Unit, Major Cyber Crimes Intelligence Unit, Middle East Intelligence Unit, and Technology Cyber Intelligence Unit.

[8] [redacted]

Office of the Inspector General Audit Approach

In August 2015, the Office of the Inspector General (OIG) initiated an audit to assess the FBI's cyber threat mitigation strategy. During initial audit work, the OIG determined that cyber threat prioritization and resource allocation was a vital precursor to mitigating cyber threats. As a result, we refined the audit objective to assess how the FBI prioritizes cyber threats.

The scope of our audit focused primarily on FBI Cyber Division's prioritization efforts and resource allocation for FY 2014 through FY 2016. The audit team interviewed 40 FBI officials, including individuals from the FBI's Cyber Division, Directorate of Intelligence, Inspections Division, Office of General Counsel, and Resource Planning Office. In addition, we interviewed a former FBI official who was the Assistant Director of the FBI Cyber Division at the time the CTT model and Threat Examination and Scoping (TExAS) tool were implemented. We conducted fieldwork at the Pittsburgh, San Antonio, and Washington Field Offices and the FBI's Cyber Initiative and Resource Fusion Unit co-located at the National Cyber Forensics Training Alliance (NCFTA). We interviewed the Director of Operations at the NCFTA and also interviewed officials from the Air Force Office of Special Investigations and the National Security Agency to gain their perspective on cyber threat prioritization. The results of our review are detailed in the Findings and Recommendations section of this report. See Appendix 1 for further discussion of the audit objective, scope, and methodology.

FINDINGS AND RECOMMENDATIONS

The FBI uses an enterprise-wide Threat Review and Prioritization (TRP) process for operational divisions to annually prioritize threats. However, because the criteria used in the TRP process are subjective and open to interpretation, we determined that the FBI's TRP process does not prioritize cyber threats in an objective, data-driven, reproducible, and auditable manner. In addition, because TRP is conducted annually, we found that TRP may not be agile enough to identify emerging cyber threats in a timely manner. To augment the TRP process, the Cyber Division developed the Threat Examination and Scoping (TExAS) tool, which uses a largely objective, data-driven, and auditable algorithm to prioritize cyber threats. In addition, if used to its fullest capability, TExAS can be updated frequently and aid in identifying emerging threats. However, we found that the use of TExAS has been uneven because the FBI has not established permanent written policies and procedures establishing how TExAS should be used in relation to the TRP and who should be responsible for entering data into TExAS. The potential to integrate TExAS with Sentinel, the FBI's case management system, may resolve some of the procedural issues by automatically updating TExAS. Lastly, we found that the FBI is not able to adequately track agent resource utilization by threat because time utilization is tracked by case classification code, and some case classification codes include multiple threats. Without the ability to track the time agents spend by threat, the FBI cannot be sure that it is aligning its cyber resources to its highest priority threats, a vital capability for a threat-driven organization.

Threat Review and Prioritization

In FY 2010, the FBI began to develop its TRP process and implemented TRP in FY 2012. TRP is a standardized prioritization process for the FBI's operational divisions to align their resources against the most severe and substantial threats.[9] The TRP process is conducted on an annual basis by both FBI headquarters and the field offices. The TRP results are entered into the FBI Resource Planning Office's Integrated Program Management tool.[10] The Cyber Division uses the Integrated Program Management tool to select the appropriate impact and mitigation levels agreed upon through its TRP sessions. The final output for the TRP process is the

[9] FBI operational divisions include the Counterterrorism Division, the Counterintelligence Division, the Criminal Investigative Division, the Cyber Division, and the Weapons of Mass Destruction Directorate.

[10] The Integrated Program Management tool is an application where FBI headquarters and field office TRP is memorialized. The IPM tool also generates documents and reports, including each field office's mandatory TRP actions and TRP results.

Consolidated Strategy Guide, which documents the annual prioritization of the FBI headquarters operational division's threats.

The Consolidated Strategy Guide is intended to ensure that everyone understands the NTPs and other program priorities. This also allows FBI headquarters to gain an understanding of threats within each field office's area of responsibility and the distribution of threats across the domestic landscape prior to determining the succeeding year's NTPs.

As part of the Cyber Division's TRP process, threats are assembled into a single, comprehensive Master Threat Issue List, which is maintained by the FBI Directorate of Intelligence. After the Master Threat Issue List is compiled, operational divisions prepare for TRP meetings by gathering documentation such as case summaries and reviews, raw intelligence reporting, finished intelligence products, and threat mitigation strategies.

After documentation has been compiled, each threat issue is discussed individually and prioritized. Participants discuss each threat issue in terms of two sets of prioritization criteria: the impact level of the threat and the mitigation level needed to address it, both as described in detail below. As shown in Table 1, the FBI uses a Threat Issue Matrix to place each threat into one of six threat bands.[11] All threat issues rated as impact Level 1 and mitigation Level A are ranked as Band I threats and designated NTP. Cyber Division threats banded between I-IV are considered severe, substantial, elevated, or guarded. Band I threats are severe, band II are substantial, band III are elevated, and band IV are guarded. There is no Cyber Division designation for threats banded as V or VI.

[11] Threat bands are risk-based prioritized tiers to which particular threat issues are assigned, based on the TRP impact level and mitigation level criteria. According to the FBI, threat bands help minimize debate in prioritization because threat issues do not have to be assigned a unique rank number and also provide for greater standardization of actions because it is easier to define expectations for a few bands than for multiple ranked threat issues. All threats within the same band level, across operational programs, are considered by the FBI to be of equal priority.

Table 1

Threat Issue Matrix

	Impact Level				
Mitigation Level		Level 1	Level 2	Level 3	Level 4
	Level A	I	II	III	IV
	Level B	II	III	IV	V
	Level C	III	IV	V	VI

Source: OIG based on information provided by FBI

We found that while decisions about each threat's impact and mitigation level made during the Cyber Division's TRP sessions were memorialized in the Integrated Program Management tool and the Cyber Division's annual Consolidated Strategy Guide, the specific information to support each threat's impact level and mitigation level was not documented. We did note that the Cyber Division provided information on the scope of the threat within the Consolidated Strategy Guide for each threat.

The FBI's Directorate of Intelligence (DI) manages the TRP process and publishes standard guidance for the operational divisions and field offices to use, including the criteria for the impact level of the threat and the mitigation resources needed to address the threat. The FBI impact level criteria attempt to measure the likely damage to U.S. critical infrastructure, key resources, public safety, U.S. economy, or the integrity and operations of government agencies in the coming year based upon FBI's current understanding of the threat issue. Impact level criteria seek to represent the negative consequences of the threat issue, nationally.

The impact level criteria include: (1) these threat issues are likely to cause the **greatest** damage to national interests or public safety in the coming year; (2) these threat issues are likely to cause **great** damage to national interests or public safety in the coming year; (3) these threat issues are likely to cause **moderate** damage to national interests or public safety in the coming year; or (4) these threat issues are likely to cause **minimal** damage to national interests or public safety in the coming year (FBI emphasis added).[12] One FBI official told us that these impact

[12] On May 2, 2016, the OIG conducted an exit conference with the FBI to discuss a draft of this report. After the exit conference, the FBI provided the OIG with documentation that demonstrated it updated its TRP impact level criteria, effective March 17, 2016, after audit work had concluded. The updated impact level criteria, which does not affect this report's findings, states: (1) these threat issues are likely to cause the **most severe** damage to national interests or public safety in the coming year; (2) these threat issues are likely to cause **severe** damage to national interests or

criteria questions, which are developed and controlled by the Directorate of Intelligence, are designed to be interpreted by the operational divisions.

The three levels of mitigation criteria, which also are standard across the FBI, measure the effectiveness of current FBI investigative and intelligence activity based upon the following general criteria: (1) effectiveness of FBI operational activities; (2) operational division understanding of the threat issue at the national level; and (3) evolution of the threat issue as it pertains to adapting or establishing mitigation action.[13]

While the criteria are standardized, we found that they were inherently subjective. One FBI official told us that the prioritization of the threats was essentially a "gut check." Other FBI officials told us that the TRP is vague and arbitrary. The Cyber Division Assistant Director told us that the TRP criteria are subjective and assessments can be based on the "loudest person in the room."

An example of the impact of the subjectivity of the ranking of threats and mitigation levels under the TRP occurred during the FY 2016 TRP process.

[redacted]

public safety in the coming year; (3) these threat issues are likely to cause **substantial** damage to national interests or public safety in the coming year; or (4) these threat issues are likely to cause **limited** damage to national interests or public safety in the coming year (FBI emphasis added). According to the FBI, the impact criteria language was modified as a result of inconsistencies identified by the Directorate of Intelligence.

[13] After the May 2, 2016 exit conference, the FBI provided the OIG with documentation that the Deputy Director approved the removal of the criteria language "*evolution of the threat issue as it pertains to adapting or establishing mitigation action.*" According to the FBI, the removal of the mitigation criteria language was intended to encourage the integrity of the process and to prevent threats from being banded higher than they should be. The removal of this mitigation level criteria, which does not affect the findings contained in this report, became effective on March 17, 2016.

[14] [redacted]

[redacted][15]

While we view the FBI's efforts to prioritize threats across the enterprise as a vital step in the mitigation process, we believe that TRP's subjective terminology is a substantial weakness in the FBI's efforts at prioritizing cyber threats. Because the criteria used in the TRP process are subjective and open to interpretation, we determined that the FBI's TRP process does not prioritize cyber threats in an objective, data-driven, reproducible, and auditable manner. We believe that the Cyber Division's threat prioritization process should rely on objective, data-driven criteria and should produce auditable rankings. Furthermore, we believe that because the TRP is a subjective process, cyber threats that require the greatest resources may not receive the highest priority.

Threat Examination and Scoping Tool

The Cyber Division must continually prioritize known and emerging threats because cyber actors adapt and alter their tactics and techniques rapidly. According to the FBI, the collaborative prioritization of threats is crucial to the successful implementation of the Cyber Division's CTT model, which is intended to enable each field office to focus on specific, assigned threats. As a result, in February 2014, the Cyber Division began developing the TExAS model, a prioritization framework tool. According to the FBI, TExAS is a software tool that (1) assesses the global cyber threat landscape and the impact of the FBI's response to those threats in an agile, transparent, and auditable manner; (2) aligns those assessments with the Cyber Division's CTT model; and (3) informs the creation of FBI's Master Threat Issue List.

Using an algorithm and a series of 53 weighted questions, the TExAS tool assigns each threat a numerical score with the most severe threats receiving the highest scores. According to its draft Cyber Division Policy Guide, the Cyber Division will require the use of the TExAS algorithm to assist the Cyber Division TRP process by providing an objective, data-driven, prioritization of cyber threats.[16]

Unlike the responses provided for the TRP impact levels, each answer provided in TExAS must be supported by a document demonstrating the underlying rationale for the answer. The questions in TExAS are intended to be objective and auditable. For example, one question asks the user whether there is evidence of

[15] We did not receive any documentation indicating that the Field Office lost any resources to address this threat as a result of it being downgraded from a NTP to a substantial threat.

[16] As of March 2016, the draft FBI Cyber Division Policy Guide had not been finalized. According to the FBI, the draft policy guide has been under final review since October 22, 2015. An estimated date for final publication was unknown at the time this report was drafted.

disruption or destruction of nuclear powered electricity and energy production and transmission systems or resources that facilitate those functions. However, we found that some questions, which appear to be adopted from Presidential Policy Directive 21 (PPD-21) – Critical Infrastructure Security and Resilience, do not contain the definitions necessary to inform the user about the criteria for making accurate selections.[17] For example, one question asks whether the target is a small business, but does not define what constitutes a small business.

We were told by the FBI official who developed TExAS that some questions were initially designed to cover the overarching critical infrastructures as defined by PPD-21 and other questions mirrored information from the National Security Council's Critical Incident Severity Schema.[18] That same FBI official explained that clarity had not been provided by the Cyber Division to further define the terminologies. In instances where definitions could be made clearer for the user, we were told that the FBI would work to create definitions and clearer language in TExAS. Because the development of the TExAS tool is not fully mature, we did not take issue with the questions and definitions; however, we believe for the FBI to maximize the benefit of TExAS, the FBI needs to ensure that the questions and potential responses are adequately defined.

According to FBI officials, TExAS has the capability to include intelligence from other agencies, the United States Intelligence Community, private industry, and foreign partners to inform FBI's prioritization and strategy. For example, a response in TExAS can be supported with documentation from a United States Intelligence Community partner for a threat as to which the FBI lacks visibility. The tool also is capable of providing data visualizations, which can help inform FBI decision makers about prioritizing or otherwise allocating resources toward new national security cyber intrusion threats, or towards national security intrusion threats where more intelligence is needed.

The TExAS tool was cited in the 9/11 Review Commission's March 2015 report as a possible best practice within the FBI.[19] Specifically, the 9/11 Review Commission stated that TExAS is "uniform and objective-based across all computer intrusion threats." Additionally, TExAS allows FBI management to prioritize or otherwise allocate resources towards emerging intrusion sets, or intrusion sets that the FBI has limited intelligence on today, to prepare for the future. According to

---

[17] Issued on February 12, 2013, PPD 21 advances a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure. PPD 21 directs the Executive Branch to develop a situational awareness capability that addresses both physical and cyber aspects of how infrastructure is functioning in near real-time.

[18] The Critical Incident Severity Schema is used to support and inform interagency coordination efforts by cyber centers, departments and agencies, including the FBI, with a cyber mission, and the National Security Council (PPD-1) system. We did not assess the Schema, or interagency coordination in response to cyber threats, as part of this review.

[19] 9/11 Review Commission, *The FBI: Protecting the Homeland in the 21st Century*, (March 2015).

the 9/11 Review Commission, the FBI intended to have the CTTs update the threat information in TExAS every 30 days.

In addition to our concerns about the clarity of some of the definitions for some of the questions TExAS asks, we also have concerns about the FBI's plan for updating TExAS every 30 days as cited by the 9/11 Review Commission. We found that, a year after the 9/11 Review Commission's March 2015 report, the FBI still had not clearly defined the roles and responsibilities for updating TExAS. In its initial iteration, one Supervisory Special Agent and one Computer Scientist managed TExAS, including entering all of the data and supporting documents for all of the threats. For FY 2016, the same Supervisory Special Agent and Computer Scientist managed the TExAS application, but the Cyber Intelligence Section entered all of the data into TExAS. In January 2016, we were told that management of TExAS was shifting from the Cyber Division's Cyber Operations Section IV to the Cyber Intelligence Section and various CTTs were conducting a pilot where they entered the data for relevant threats into TExAS from field offices around the country ahead of the FY 2017 TRP process.[20]

Since its implementation, the TExAS tool has been managed without documented policies and procedures detailing the roles and responsibilities for entering data about each threat. While several electronic communications have been issued to coordinate efforts and advise stakeholders of enhancements to TExAS, the Cyber Division has not issued a policy directive, in draft or final, describing: (1) who is responsible for managing TExAS' questions and answers or its algorithm, (2) who is responsible for entering data into TExAS, (3) how frequently TExAS data should be updated, or (4) how TExAS results should be reconciled with the results of the TRP process. FBI officials told us that this has resulted in confusion about responsibilities, infrequent data entry, and inconsistent prioritization results. We believe that the FBI should document policies and procedures and provide training for the use of the methodology, including who should enter the data, how frequently, and how the data should be used in prioritizing cyber threats.

As discussed previously, program management of the FBI prioritization process resides in the Directorate of Intelligence, which also sets the FBI Intelligence Program priorities and manages the intelligence functions within the FBI. During our audit work, an FBI official told us that the weighted questions that comprise TExAS must be approved by the Cyber Intelligence Section because the Directorate of Intelligence is responsible for the prioritization process.

---

[20] The Cyber Operations Section IV is a headquarters based section responsible for enabling, supporting, and coordinating FBI global cyber operations. One of the roles of the Cyber Operations Section IV is to provide the Cyber Division with the resources and expertise to create flexible, rapid-response operational capabilities specifically designed to address the operational requirements of all of the Cyber Division's threat units.

[redacted] The only variable that changed substantially in TExAS and TRP between FY 2015 and FY 2016 was who entered the data into TExAS. Given the subjectivity of the TRP process, we cannot conclude that the relative lack of alignment between TExAS and TRP is bad in itself. However, we believe other factors concerning the implementation of the TExAS tool contributed to the size of the discrepancy. FBI officials told us that inputting data into TExAS has been an uneven administrative burden for some units, and that a lack of clearly defined roles and responsibilities for proper input of information into the TExAS tool, and limitations of the TExAS tool might have contributed to the difference in the TRP and TExAS results.

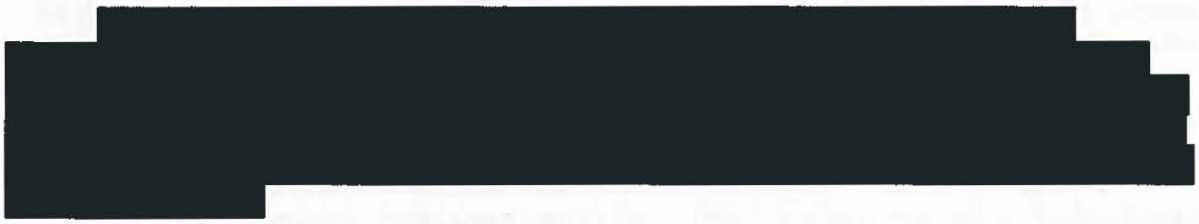
As an example, for the FY 2016 TExAS banding, the units that comprise of the Cyber Intelligence Section entered the information for the threats they covered into the TExAS tool. [redacted].[21] While TExAS represents an opportunity to score threats objectively, the administrative burden of manually entering sufficient data is a challenge for the Cyber Division.

While we believe that the TExAS tool is not fully mature, and the results it produces are only as good as the data entered into it, we believe that the Cyber Division's development of the TExAS tool is a best practice, which also may have applications for the other FBI operational divisions. We believe that as cyber threats continue to increase in size and complexity, the FBI's ability to effectively prioritize the most serious threats will increasingly require objective, data-driven means of assessing the severity of threats. The use of a data-driven, objective, and auditable methodology to scope and prioritize cyber threats provides the FBI with a reproducible prioritization process. While TExAS currently is designed to augment the Cyber Division's TRP process, we believe its methodology could streamline the prioritization process in other operational divisions as well.

[21] In February 2016, an FBI official told us that TExAS has been upgraded to enable users to indicate the presence of documentation at higher classification levels.

Timeliness in Prioritizing Emerging Cyber Threats

Because TRP is an annual process, it may not be frequent enough to handle emerging cyber threats, which receive little emphasis in the TRP process. The cyber threat landscape changes quickly as cyber actors develop new tactics and techniques to counter the responses taken by the private sector, the FBI, and the other agencies involved in countering cyber threats. However, FBI officials told us that it is difficult to act on cyber threats not ranked in the top bands because even the highly ranked threats do not have the appropriate resources. While we commend the FBI for prioritizing the threats it ranks to be the most severe, we believe that the FBI's prioritization needs to be agile enough to consistently spot emerging threats during the intervals between the annual TRP process.



As discussed previously, the draft Cyber Division policy will require that the TExAS application support the TRP process. TExAS is more objective than TRP and, if properly implemented, can prioritize threats more frequently and more efficiently than TRP. A Cyber Division official told the OIG that it intends to have Sentinel, the FBI's case management system, automatically update TExAS with available data once a day in FY 2017 and to have the applicable CTT field offices manually enter the data that Sentinel cannot transfer every 30 days. The 9/11 Review Commission stated that the "real-time updates represent a useful augmentation to the TRP because it allows for transparency – intelligence analysts and decision-makers can clearly visualize the threats – and it also indicates new [emerging] and/or adapting threats." The 9/11 Review Commission also noted that, under the current system, once Cyber Division resources are allocated under the annual TRP process, the division had to scramble to reallocate existing resources to address any newly-identified threats.

If integrated with Sentinel, we believe that the TExAS tool has the potential to provide a current picture of the threat landscape. According to an FBI Sentinel official, interfacing TExAS with Sentinel would not be difficult because the interface design already exists. Sentinel integration would assist the Cyber Division in overcoming the burden of manually updating the tool.

We believe that TExAS should be designed to provide updates to the Cyber Division at least every 30 days in order to identify emerging threats and adapting known threats. If emerging threats are not identified or addressed in a timely manner, the FBI may well not be allocating appropriate resources to significant emerging cyber national security matters.

Tracking the Utilization of Investigative Resources

As a related matter, we found, and the FBI acknowledged, that it is not currently possible to track the resources allocated to each cyber threat. As described above, all of the FBI's operational divisions use the TRP process to prioritize the threats for which they are responsible, and the Cyber Division uses the CTT model to assist in allocation of resources by threat. For example, all severe (or NTP) and substantial threats must be assigned to a Strategic Threat Execution office. Severe threats are also allocated up to two dedicated Cyber Division Supervisory Special Agent Threat Managers at headquarters, at least one of which is an experienced Cyber Agent. However, the FBI currently tracks its agents' investigative efforts using its Time Utilization and Recordkeeping (TURK) system. TURK is a process within the FBI's WebTA system and is unable to track agents' effort on a specific threat.[22] Agents using TURK record their proportion of time spent on various case classification codes, not the threats that they are investigating. Because the FBI cannot track resources dedicated to each threat, it cannot ensure that resources are being applied to threats appropriately.

During our fieldwork, we determined that multiple threats use the same classification code, and case classification codes generally remain static from year to year while threats change yearly. [redacted] According to the FBI, for those classifications with multiple threats, it is impossible to use TURK data to measure the amount of resources allocated to a threat, and the FBI does not have any other measure of agent time that would address this. We were told by an FBI official that TURK data may be used in cases where only one threat is associated with a given case classification, a circumstance that is likely only for lower priority threats.

Hence, while the FBI prioritizes its efforts and resources by threat, it has no way to track the resources it expends addressing each threat. We discussed the issue with FBI officials who acknowledged the issue, and we were told that they are working on a solution. The FBI officials told us that several interrelated systems would need to be updated in order to use TURK data to measure the resources allocated to threats. In addition, the same FBI officials told us that because classification codes do not align to threats, there would be historical data implications to updating the TURK system to track time utilization by threat. We believe the FBI should develop and implement a record keeping system that tracks agent time utilization by threat. Without the ability to track the time agents spend by threat, the FBI cannot be sure that it is appropriately aligning its cyber resources

[22] WebTA is the FBI's web-based system to record time and attendance data. While all FBI employees use WebTA, only operational employees must utilize the FBI TURK system to track their time. For agents, only non-management field agents TURK. In addition, non-agent positions may TURK, including Intelligence Analysts, Computer Scientists, and Financial Analysts.

to its highest priority threats, a vital capability for a threat-driven organization in the current cyber climate.

Conclusion

We found the criteria used in the TRP process are subjective and open to interpretation. As a result, the FBI's TRP process does not prioritize cyber threats using an algorithmic, objective, data-driven, reproducible, and auditable manner. In addition, we found that TRP may not be agile enough to identify emerging cyber threats. We believe that as cyber threats continue to increase in size and complexity, lack of objective, data driven prioritization can hinder the FBI's ability to effectively prioritize the most serious threats. The Cyber Division's newly developed TExAS tool, used in conjunction with the existing enterprise-wide TRP process, offers the FBI a data-driven, objective, and auditable methodology capable of scoping and prioritizing cyber threats. However, we found that TExAS lacks written policies and procedures outlining data entry and how the data should be used in prioritizing threats.

If the FBI achieves its intended integration with Sentinel, we believe that TExAS, or a system of similar ability, has the potential to provide a current picture of the cyber threat landscape, including emerging cyber threats as well as known threats that are adapting techniques, tactics, and procedures that receive little emphasis in the annual FBI TRP process. While we recognize that any system is only as good as the data entered into it, we believe an application like TExAS, is a best practice that could streamline the prioritization within the Cyber Division and potentially across other FBI operational divisions.

Additionally, we found that the FBI is not able to adequately track agent resource utilization by threat. As a result, the FBI cannot be sure that it is aligning its cyber resources to the highest priority threats. We believe the FBI should develop and implement a record keeping system that tracks agent time utilization by threat.

The FBI has taken significant steps towards prioritizing the cyber threats it must address. We believe that greater reliance on objective and auditable information in the threat ranking process will enhance the FBI's ability to accurately and efficiently prioritize cyber threats and direct resources accordingly. A key requirement for a threat driven organization is the ability to track resources according to threat, and we find that the FBI can improve in this area.

Recommendations

We recommend that the FBI:

1. Utilize a algorithmic, data-driven, and objective methodology in the scoping and prioritization of cyber threats, including:

    - Document policies and procedures and provide training for the use of the methodology, including who should enter the data and how the data should be used in prioritizing cyber threats.

    - Ensure that the results of the threat ranking tool are updated automatically through integration with Sentinel and updated manually at least every 30 days so that emerging threats can be identified and mitigated in a timely manner.

2. Develop and implement a record keeping system that tracks agent time utilization by threat.

STATEMENT ON INTERNAL CONTROLS

As required by the *Government Auditing Standards*, we tested, as appropriate, internal controls significant within the context of our audit objectives. 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 Federal Bureau of Investigation's (FBI) 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.

As noted in the Findings and Recommendations 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 adversely affect the FBI's ability to effectively prioritize cyber threats and adequately track agent resource utilization by threat.

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.

STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS

As required by the *Government Auditing Standards* we tested, as appropriate given our audit scope and objectives, selected transactions, records, procedures, and practices to obtain reasonable assurance that the Federal Bureau of Investigation's (FBI) 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 objectives:

- Executive Order 13636

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. Nothing came to our attention that caused us to believe that the FBI was not in compliance with the aforementioned laws and regulations.

APPENDIX 1

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The preliminary objective of our audit was to assess the FBI's cyber threat mitigation strategy. During preliminary fieldwork, we determined that each cyber threat may have a different threat mitigation strategy. In order for the FBI to develop a strategy for each cyber threat, the FBI must prioritize threats and allocate resources to each threat. As a result, we refined our audit objective to assess how the FBI prioritizes cyber threats.

Scope and Methodology

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 objectives.

Our audit focused on the FBI Cyber Division's threat prioritization efforts and related resource allocation to each threat. The scope of our review encompassed the Cyber Division's prioritization and resource allocation from FY 2014 through FY 2016.

To accomplish our audit objective, we interviewed 40 FBI officials, including individuals from the FBI's Cyber Division, Directorate of Intelligence, Inspections Division, Office of General Counsel, and Resource Planning Office. In addition, we interviewed the former Assistant Director of the Cyber Division in place during the scope of our audit. We conducted fieldwork at the Pittsburgh, San Antonio, and Washington Field Offices and the FBI's Cyber Initiative and Resource Fusion Unit co-located at the National Cyber Forensics Training Alliance (NCFTA). We interviewed the Director of Operations at the NCFTA and also interviewed officials from the Air Force Office of Special Investigations and the National Security Agency to gain their perspective on cyber threat prioritization.

To gain a better understanding on the Cyber Division's prioritization efforts and related resource allocation to threats, we reviewed the draft version of the Cyber Division Policy Guide and the TURK Policy Directive. We also reviewed FBI's policies and guidance related to intelligence programs and products. In addition, we reviewed and began evaluating planning documentation and reports on the TExAS tool.

APPENDIX 2

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

June 30, 2016

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

Dear Mr. Horowitz:

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 Threat Prioritization*.

We are pleased that you found, "The FBI has taken significant steps towards prioritizing the cyber threats it must address."

We agree that it is important to both utilize objective information in the threat ranking process and implement a system that allows for tracking agent time utilization by threat. In that regard, we concur with your two recommendations for the FBI.

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

Sincerely,

James C. Langenberg
Section Chief
External Audit and Compliance Section
Inspection Division

Enclosure

The Federal Bureau of Investigation's Response to the
Office of the Inspector General's Audit of the FBI's Cyber Threat Prioritization

Report Recommendation #1: (U) Utilize an algorithmic, data driven, and objective methodology in the scoping and prioritization of cyber threat sets, including:

- Document policies and procedures and provide training for the use of the methodology, including who should enter the data and how the data should be used in prioritizing cyber threat sets.

- Ensure that the results of the threat ranking tool are updated automatically through integration with Sentinel and updated manually at least every 30 days so that emerging threat sets can be identified and mitigated in a timely manner.

FBI Response to Recommendation #1: Concur. Policies are currently being drafted which will include identifying the parties responsible for maintaining and managing the development of TExAS, as well as who will be responsible for entering data into TExAS. We've begun drafting a communications plan to inform end users about the coming changes to TExAS and educating them on the purpose and use of the tool.

TExAS will continue to serve as a starting point for discussions on the ranking of cyber threats. Given the classification limitations of TExAS, rankings in TExAS will be supplemented by the expertise of analysts and investigators to determine final rankings of cyber threats.

FBI Cyber Division is also currently working with the Sentinel development team in the Information Tech Applications and Data Division to integrate TExAS functionality into the Sentinel document creation process. Once Sentinel/TExAS integration has been completed, policy guidance will be provided to the field from Cyber Division clearly stating expectations regarding how frequently records should be entered into TExAS to ensure threat rankings are updated at least every 30 days.

Report Recommendation #2: (U) Develop and implement a record keeping system that tracks agent time utilization by threat set.

FBI Response to Recommendation #2: Concur. The FBI concurs with the need to develop and implement a record keeping system that tracks agent time and utilization by threat. The FBI has assembled a team to begin analyzing the data, process, reports, workload, and IT systems requirements that would be impacted by the proposed change.

APPENDIX 3

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

The OIG provided a draft of this audit report to the Federal Bureau of Investigation (FBI). The FBI's response is incorporated in Appendix 2 of this final report. The following provides the OIG analysis of the response and summary of actions necessary to close the report.

Recommendation:

1. **Utilize an algorithmic, data driven, and objective methodology in the scoping and prioritization of cyber threat sets, including:**

   - **Document policies and procedures and provide training for the use of the methodology, including who should enter the data and how the data should be used in prioritizing cyber threat sets.**

   - **Ensure that the results of the threat ranking tool are updated automatically through integration with Sentinel and updated manually at least every 30 days so that emerging threat sets can be identified and mitigated in a timely manner.**

   Resolved. The FBI concurred with our recommendation. In its response, the FBI stated that policies are being drafted that identify the parties responsible for maintaining and managing the development of TExAS, including who should be responsible for entering data into TExAS. The FBI also stated that TExAS will continue to serve as a starting point for discussions on the ranking of cyber threats and will be supplemented by the expertise of analysts and investigators to determine final rankings of cyber threats. In addition, the FBI stated that the Cyber Division is currently working with the Sentinel development team to integrate TExAS functionality. According to the FBI, once the integration is completed, policy guidance will be provided from the Cyber Division clearly stating expectations to ensure threat rankings are updated at least every 30 days.

   This recommendation can be closed when we receive evidence that the FBI is utilizing an algorithmic, data driven, and objective methodology in the scoping and prioritization of cyber threat sets; documenting relevant policies and procedures; providing training for the use of the methodology; and ensuring that the results of its threat ranking tool are updated at least every 30 days.

2. **Develop and implement a record keeping system that tracks agent time utilization by threat set.**

Resolved. The FBI concurred with our recommendation. In its response, the FBI stated that it has assembled a team to begin analyzing the data, process, reports, workload, and IT systems requirements that would be impacted by implementing a system that tracks agent time and utilization by threat set.

This recommendation can be closed when we receive evidence that the FBI has developed and implemented a record keeping system that tracks agent time utilization by threat set.

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. Information may be reported to the DOJ OIG's hotline at www.justice.gov/oig/hotline or (800) 869-4499.

Office of the Inspector General
U.S. Department of Justice
www.justice.gov/oig