UNITED STATES DEPARTMENT OF COMMERCE
Office of the General Counsel
Washington, D.C. 20230

Report of the Programmatic Review of the Investigations and Threat Management Service

September 3, 2021

On March 2, 2021, the Department of Commerce (Department) received the Department of Commerce Office of Inspector General's Report of Investigation (OIG ROI) No. 19-0714 concerning the Investigations and Threat Management Service (ITMS). The OIG ROI addressed certain allegations of misconduct and abuse of authority. Based on a review of the OIG ROI, on April 19, 2021, the Department commissioned a broader programmatic review of ITMS's operations to identify and propose solutions for any substantiated management or operational deficiencies (the Review). The Review, undertaken by Office of the General Counsel personnel and an agent from the Bureau of Industry and Security's Office of Export Enforcement (the Review Team), began on April 26, 2021. This report is the result of the Review. The Department has also provided this report to the Office of Inspector General (OIG) in response to OIG ROI No. 19-0714.

Executive Summary

The Department must provide security for its people, operations, information, and property. As part of that mission, the Department's Office of Security (OSY) in 2006 established the unit that evolved into the Investigations and Threat Management Service. OSY conceived of ITMS as a specialized unit to centralize investigative capabilities. The stated purpose of the unit is to conduct investigations and analyses to identify, assess, mitigate, or prevent critical threats to the Department's mission, operations, or activities. ITMS has housed a series of investigative functions to address threats to the Department. Chief among these are criminal law enforcement investigations, administrative investigations of security violations or risks, protective intelligence investigations concerning threats to the Secretary, insider threat detection, and purported "counterintelligence" investigations. The Department designates ITMS personnel as criminal investigators, a designation that requires the agents to spend at least 50% of their time on the criminal investigative component of the mission. There were 11 criminal investigators in ITMS at the start of the Review. In sum, ITMS is responsible for addressing threats to the Department through various types of investigations, with an emphasis on criminal law enforcement investigations.

The purpose of the Review was to assess the overall practices, policies and performance of ITMS in fulfilling its mission and to recommend whether ITMS as a program should continue in its current, or in an alternative, form. The Review Team conducted dozens of interviews, reviewed hundreds of documents, and analyzed relevant legal authorities. The Review Team has concluded that the Department should discontinue performing certain of ITMS's functions, reassign its remaining functions to other Department components and eliminate ITMS.

The Department's law enforcement and intelligence authorities do not include the full scope of the criminal law enforcement and counterintelligence authority that ITMS claimed to exercise. And in practice, few ITMS investigations relied on this authority. To date, the Review Team has

found only two investigations that resulted in criminal charges and has not found evidence indicating that ITMS relied upon counterintelligence authorities. Accordingly, the Department should end the criminal law enforcement or counterintelligence missions that ITMS sought to perform.

ITMS's primary remaining functions—chiefly, administrative security investigations, protective intelligence, and insider threat detection—rest on firmer legal grounds. The Department should retain these functions. The Department, however, does not need to aggregate these functions in a single unit. It can assign them to other offices with relevant subject matter expertise. Administrative investigations into the mishandling of classified information, for example, can be assigned to the Department's Information Security Division, which already has responsibility for safeguarding this information. The Deputy Assistant Secretary for Intelligence & Security (DAS-IS) should develop and execute a detailed plan for transferring these remaining functions.

The Review Team further recommends that the Department update the policies, procedures, training, and oversight framework for the remaining functions that will continue in other units. The Department should ensure it has written policies for administrative security investigations, protective intelligence investigations, and insider threat detection that comply with all applicable laws and ensure that adequate safeguards exist to protect privacy, civil rights and civil liberties. Privacy, civil rights, civil liberties, and legal authority generally should be the subjects of regular trainings for the personnel involved in administrative security investigations, protective intelligence, or insider threat detection. The Department should also implement oversight mechanisms for its administrative security investigations and insider threat activities that include a role for experts in civil rights and civil liberties, privacy, and relevant legal authorities.

The Review Team has provided information to Department management for appropriate personnel actions. Such actions are the decision of Department management, not the Review Team, and the actions taken cannot, by law, be disclosed in this report. Separately, discontinuing the criminal law enforcement function of ITMS means that ITMS agents cannot remain within the Office of Intelligence and Security (OIS) as criminal investigators. The Department must address this situation consistent with federal employment law. That process will be communicated to the impacted employees.

The Department must also address case management issues as part of the orderly elimination of the ITMS program. ITMS has many open cases. The Review Team has begun work to review those open cases and to close those that do not need to be continued. Based upon the review to date, the Review Team expects the overwhelming majority of the open cases will be closed. The Department should continue this case review, archive the case files, and establish an appropriate schedule for the destruction of this information that complies with applicable law. If the review of case files results in the identification of any potential misconduct that has not already been addressed, that information should be provided to Department management for proper resolution.

Many Department employees have expressed concerns about whether they were the subject of an ITMS investigation. Addressing these concerns is important. For that reason, the Review Team recommends that the Department implement policies to ensure that no information developed by ITMS informs future Departmental decisions without prior legal review and independent corroboration. In addition, the Department should advise employees of their legal rights to access information under the Privacy Act and Freedom of Information Act, and to request corrections to their personal information.

Four sections follow. The first provides background on the Review. The second provides background on ITMS. The third presents the Review's findings. The fourth contains the Review's recommendations.

I. Review Background

A. Review Scope

The OIG ROI grew out of a complaint received by the OIG in June 2019. The OIG ROI was not a programmatic review, but it included evidence of potential misconduct and mismanagement within ITMS occurring over several years. The Department determined that a programmatic review of ITMS was needed to address the issues raised in the OIG ROI. The Department's Chief of Staff ordered the Review on April 19, 2021.

The Office of the General Counsel (OGC) led the programmatic review. A team of attorneys and a supervisory law enforcement special agent from the Bureau of Industry and Security's Office of Export Enforcement performed the Review.

The scope of the Review was to address:

- whether ITMS cases were being opened and pursued with proper legal authority and factual predicates and brought to timely resolution;
- whether there were gaps or needed updates in policies, procedures, and training, with recommendations to implement any curative updates or new policies or training; and
- an analysis of the work that ITMS has done to date, including case closure rates and an assessment of an appropriate process establishing investigative priorities that can be supported by existing authorities and budget.

Members of the Review Team interviewed 47 people, including current and former ITMS and OSY employees, subjects of ITMS investigative activities, current and former Department managers in the Office of the Chief Financial Officer and Assistant Secretary for Administration, and attorneys in OGC.

The Review Team collected and reviewed documents going back to the earliest days of ITMS. It collected information on ITMS cases and reviewed various case files to develop an understanding of ITMS's operations and to address specific concerns raised about ITMS activity. Complicating the Review was the fact that ITMS's case files are not well-organized. The Review Team began a separate project to collect, organize, and archive all ITMS case files. That project is ongoing.

The Review Team also considered the OIG's findings regarding ITMS and the report on ITMS published by the minority of the U.S. Senate Committee on Commerce, Science & Transportation.

B. Other Department Actions on ITMS

The Department has already taken actions to address concerns about ITMS. As a result of the Department's receipt and initial review of the OIG ROI, the Department on March 10, 2021, directed ITMS to suspend all criminal law enforcement investigations. The Department also

directed ITMS agents to immediately cease carrying weapons and to return those weapons for safekeeping in the Herbert C. Hoover Headquarters Building. The Department has secured and inventoried those weapons. Later, based on information learned during the Review, the Department suspended all ITMS investigations.

The Department has also engaged concerned employees. The Department enlisted the assistance of the Chief Ombudsman at the United States Patent and Trademark Office to respond to questions and concerns from employees and confidentially communicate those questions and concerns to senior leadership. The Department has also engaged in a listening session with and received recommendations from some employee resource groups.

II. ITMS Background

A. Origins of ITMS

In October 2006, OSY established a new central unit for conducting investigations. This is the unit that evolved into ITMS. It went by various names from its inception to today. This report refers to the unit as ITMS.

From its inception until 2019, ITMS was a component unit of OSY under the Director of Security. In late 2019 or early 2020, the Department created the position of DAS-IS and ITMS became a standalone unit reporting to the DAS-IS. The current DAS-IS joined the Department in July 2021, with this Review well underway.

B. ITMS Mission

Various departmental policies describe ITMS. Department Organization Order 20-6, "Director for Security,"[1] section 5.02, states that ITMS is to

> conduct investigations and analyses to identify and/or assess critical threats to the Department's mission, operations, or activities; prevent or mitigate such threats from adversely affecting Department personnel, facilities, property, or assets through strategic and tactical approaches; and collaborate with other national security and law enforcement entities as appropriate.

Department Administrative Order 207-1, "Security Programs," [2] section 4.01.a.6, further states that ITMS:

> initiates and completes complex and sensitive criminal and administrative investigative functions, as well as due diligence and exploratory inquiries across varied program areas including conducting counterintelligence investigations involving personnel (e.g., foreign national visitors), classified/sensitive information and critical programs, as well as protective intelligence investigations related to the Secretary or his designees.

[1] Dep't Org. Order 20-6, § 3, *available at* https://osec.doc.gov/opog/dmp/doos/doo20_6.html.
[2] Dep't Admin Order 207-1, §4.01.a.6, *available at* https://osec.doc.gov/opog/dmp/daos/dao207_1.html.

The Department in 2014 also assigned ITMS a role in its insider-threat detection program. Based on these Departmental policies, other documents received, and interviews, the Review Team identified four main ITMS activities:

- *criminal law enforcement investigations*, which are investigations of potential criminal offenses;
- *administrative investigations*, which are investigations that relate to violations of Department policy or incidents that may threaten the security of Department personnel, information, activities, or property;
- *protective intelligence*, which involves assessing information relevant to potential threats against the Secretary and other designated Department officials; and
- *insider threat detection*, which is a required activity under law[3] and covers threats that an insider will use authorized access, wittingly or unwittingly, to do harm to the security of the United States, including through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities.

While these four activities may not encompass all of ITMS's work, the Review Team believes they are comprehensive for purposes of the Review.

C. ITMS Workforce

When ITMS was created, there were five staff members in the office. At the start of the Review, ITMS had 13 employees: 11 criminal investigators and two administrative employees. General practice is for ITMS agents to apply for Top Secret/Sensitive Compartmented Information (TS/SCI) security clearances and to seek and receive access to classified networks pursuant to standard Department procedures.

The ITMS workforce has had substantial turnover through the years. Onboard positions have fluctuated from 9 to 17 over the last five fiscal years, with an average staff of 12. Twenty-eight employees left ITMS since 2010, an attrition rate of three employees leaving per year, or about 25% of the average staff level of 12. When this Review began, six of the 11 ITMS criminal investigators had been in their roles for less than two years, including four who had been at ITMS for less than a year.

In May 2010, the then-Director of OSY requested that the Department reclassify the security specialist positions in ITMS as criminal investigators and certify that these positions met the requirements for special availability pay and retirement coverage available to law enforcement officers. These positions are the Office of Personnel Management's 1811 Criminal Investigator series. To satisfy the requirement of the criminal investigator job series, an employee must spend the majority of his or her time on criminal law enforcement investigations. In submitting the request for this change, the then-Director of OSY estimated that ITMS criminal investigator employees would spend 70% of their time on criminal investigations. The Department approved

[3] *See* Exec. Order No. 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information (Oct. 7, 2011).

this change. Because of this change, except for administrative employees, ITMS employees are criminal investigators.

ITMS is led by a director (the ITMS Director). Only one person has served as the ITMS Director in the unit's history. That person has not performed duties related to ITMS since August 2020. No new director has been appointed, though an agent has served in an acting capacity.

Several interviewees told the Review Team that the ITMS Director exercised a high degree of control over the day-to-day activities of the office. That is consistent with what interviewees told the OIG, which reported in the OIG ROI that the ITMS Director "stove-piped" everything, discouraged proactive initiatives, and refused to permit agents to make contacts outside ITMS without prior approval. Several agents reported that ITMS is a toxic work environment.

D. Snapshot of ITMS Cases

ITMS has three tiers of cases: "intake," "inquiry," or "investigation":

- An "intake" is the lowest level of matter reviewed for action by ITMS and is used for new matters referred to or developed by ITMS. Intakes often involve minimal investigative activity.
- An "inquiry" is the next case level. For an inquiry, ITMS agents determine whether a matter is not "fictitious, baseless, or improper," meets mission requirements, and is "solvable." If those conditions are met, an "inquiry" can become an investigation.
- An "investigation" is a case conducted to determine if a suspicion or allegation is substantiated.

This intake/inquiry/investigation methodology appears to be uniquely developed within ITMS. Some interviewees expressed frustration and confusion with this approach.

ITMS tracks its case in a spreadsheet which, as discussed below, may not be complete. Based on that spreadsheet, it appears that between 2015 and 2019, the number of cases that ITMS would open each year ranged from a low of 428 in 2016 to a high of 821 in 2018. These include cases of all three types listed above. In 2020, ITMS opened only 153 cases. This year, it opened only 20 cases before the Department suspended its investigative operations.

As of the time the Review began, the case tracking spreadsheet indicated that ITMS had approximately 1,945 open cases. The Review Team has been collecting information on each of these cases. That process is not fully complete (and will continue after the publication of this report). However, based on review of ITMS's case tracking spreadsheet, review of summary information developed on approximately 1,500 of the 1,945 open cases so far, and review of select case files, the Review Team can make the following observations:

First, it appears that 54 of the 1,945 open cases are "investigations" under ITMS's methodology. Of those 54, only 13 have a status update in ITMS's case management system later than January 1, 2020. The status of those 13 cases indicate that they are pending closure.

Second, the Review Team estimates that approximately 60-65% of the 1,945 open cases were "intakes," *i.e.,* the lowest form of case that involved the least amount of activity. Of these, the majority were protective intelligence intakes to process correspondence, usually directed to the

Secretary and referred to ITMS for review. That process is discussed in further detail in the section on protective intelligence.

Third, very few of the approximately 1,945 open cases had any recent investigative activity. The Review Team estimates that only 10-15% have had any activity since January 1, 2020. A third or more may not have had any activity since 2017 or earlier.

Finally, it appears to the Review Team that only a small number of ITMS's overall cases contributed to management actions against Department employees. ITMS itself did not have the authority to take employment actions against non-ITMS personnel, suspend access to classified information, or determine adequacy for security clearances. However, from interviews and case files, it appears that its work in certain instances informed Department personnel who made those decisions.

III. Findings

This section presents the Review's findings on major issues that the Department should address. These findings do not discuss all the findings of the OIG ROI. The Department is addressing findings in the OIG ROI related to specific instances of misconduct through personnel actions. These findings are also not a comprehensive statement of all the work that ITMS did and should not be used to imply any specific judgments about ITMS agents. These findings address program-level issues that rank-and-file ITMS agents did not control, and that some tried to change.

A. Evaluation of ITMS's Mission

This section assesses whether the Department requires ITMS to perform the security missions assigned to it. The Review Team concludes that it does not. ITMS's criminal law enforcement and counterintelligence missions should end. The remaining functions of ITMS should be redistributed to other units of the Department.

This section proceeds by addressing, in turn, ITMS's role in criminal law enforcement, administrative investigations, protective intelligence, insider threat detection, and counterintelligence. The Review assesses ITMS's criminal law enforcement activity in particular as that appears to have been a priority for ITMS leadership.[4]

1. Criminal Law Enforcement Investigations

ITMS did not possess adequate legal authority to investigate the array of criminal activity it sought to address. This authority is also not essential for the Department to exercise because other agencies, including the OIG and Federal Bureau of Investigation (FBI), can protect the Department against criminal activity. For these reasons, the Review Team recommends ending ITMS's criminal law enforcement investigation function.

Validity of ITMS's Criminal Law Enforcement Authority. Federal criminal law enforcement generally includes the authority to detect crimes against the United States, execute warrants and

[4] This Review relates only to the criminal law enforcement authority that ITMS sought to exercise. There are other law enforcement authorities in the Department that relate to Department offices unrelated to this Review.

make arrests, conduct criminal investigations and searches, and carry firearms. *See, e.g.*, 50 U.S.C. § 4820 (defining the Department's authority to enforce certain export control laws). No federal statute empowers ITMS to engage in criminal law enforcement activities. That is unlike other law enforcement offices within the Department (*e.g.*, the OIG, the Office of Export Enforcement in the Bureau of Industry and Security, and the Office of Law Enforcement in the National Oceanic and Atmospheric Administration), which have statutory law enforcement authority.

Despite the absence of statutory authority, the Department has claimed that ITMS has criminal investigation authority. Department Administrative Order 207-1 states that ITMS "initiates and completes complex and sensitive criminal . . . investigative functions."[5] The Department claimed this authority to conduct criminal investigations primarily on the basis of a deputation from the U.S. Marshals Service (USMS). For an individual to receive a deputation, an agency must sponsor the individual and submit certain information to USMS. USMS considers that information and grants a deputation as appropriate. This authorizes them to perform the functions of a deputy U.S. marshal, *see* 28 C.F.R. § 0.112, which includes certain law enforcement functions, *see, e.g*, 28 U.S.C. § 566(d) (authorizing deputy U.S. marshals to carry firearms and make arrests). The appointment form states that the authorities granted to a deputized agent "can only be exercised in furtherance of the mission for which he or she has been specially deputized and extend only so far as may be necessary to faithfully complete that mission." In other words, any criminal law enforcement authority conferred by the deputation is limited to the mission for which the deputation is granted.

The USMS appointment form states the purpose of the deputation. The specific wording of these duties on ITMS agent deputation appointment forms varied over time. The broadest purpose on any appointment was for "protection of the Secretary of Commerce and [the Department's] critical assets." The deputation appointment also included the words "protection detail," in all capital letters, under the ITMS agents' names. Below is an excerpt from an ITMS agent deputation, with personal identifying information removed:

[5] Dep't Admin. Order 207-1, §4.01.a.6, *available at* https://osec.doc.gov/opog/dmp/daos/dao207_1 html.

SPECIAL DEPUTATION APPOINTMENT

[redacted]

PROTECTION DETAIL

has been specially appointed as a Special Deputy U.S. Marshal
to perform the following duties as authorized by law:

* VALID WHEN PROVIDING PROTECTION FOR THE SECRETARY OF COMMERCE AND DOC CRITICAL ASSETS

This deputation has the following limitations:

* NOT AUTHORIZED TO PARTICIPATE IN FEDERAL DRUG INVESTIGATIONS UNLESS DEPUTIZED BY DEA OR FBI
* NOT VALID OFF DUTY

ITMS interpreted its authority under the deputations to protect "critical assets" to include the authority to investigate alleged criminal violations that threatened "activities or items which if compromised would cause significant damage to the U.S. Government's ability to function, U.S. economic advancement, or Departmental functions in support of these concerns." ITMS training materials stated that this investigative authority extended to a wide range of criminal offenses, including espionage, counterterrorism, organized crime, money laundering, and more. In sum, ITMS has operated under the notion that the USMS special deputation authorized ITMS to exercise criminal law enforcement authority to enforce a wide range of criminal law if enforcement somehow protected the Department's activities.

The Review Team has not been able to determine the origin of this interpretation of the USMS deputation. Regardless, ITMS and the Department should not have relied on the USMS deputation for broad-reaching criminal law enforcement authority.

ITMS and the Department failed to establish a clear understanding with the USMS on the scope of the deputation. USMS was the source of the deputation. It knew what authority it possessed and what portion of that authority it was delegating. The Review Team did not find evidence that the Department or ITMS received the clear agreement of USMS that the special deputation authorized the broad investigative mission that ITMS sought.

It is clear from the OIG ROI that the USMS does not agree with ITMS's interpretation of the deputation. USMS stated during the investigation underlying the OIG ROI that the deputation only authorized ITMS agents to carry a weapon and conduct arrests while protecting the Secretary or Department facilities or equipment. USMS also had a conversation with certain OIS and ITMS personnel in the latter half of 2020 in which they explained that the deputation did not extend to the broad array of investigations that ITMS claimed were within its mission.

It appears that the Department and ITMS may have believed the broad interpretation of the deputation was appropriate based on the letters to USMS requesting the deputation. The Review

Team reviewed the letters to USMS that it could find. The letters reviewed did discuss ITMS's mission to protect critical assets, including the Department's activities, and to conduct investigations. But in the Review Team's view, those letters did not put the USMS on clear notice that ITMS was relying on the USMS deputation for the full scope of that mission. The operative sentence requesting the deputation stated:

> Special deputation to bear firearms and exercise arrest authority while "**providing security for Department of Commerce critical assets and protection for the Secretary**" is required in order to: 1) protect critical assets and the Secretary of Commerce, as described in this document; 2) ensure assigned special agents can protect themselves and others from danger; 3) protect evidence from destruction; and 4) ensure an interim Federal presence before other duly appointed investigative and law enforcement agencies can assume any related responsibilities.

While the letters do generally describe ITMS's investigative mission, this sentence does not explicitly tie the investigation function to the deputation. Based on the information it has reviewed, the Review Team does not believe it would have been clear to USMS that a broad investigative deputation was sought.[6]

In the absence of a shared understanding with USMS on the scope of the deputation, ITMS and the Department should not have interpreted the deputations to serve as a broad delegation of criminal law enforcement authority. In the view of the Review Team, the deputations were too ambiguous to justify that interpretation. First, the deputations state in all capital letters that they are for the "Protection Detail." This is not the title one would expect for a deputation authorizing an agent to act as a criminal investigator. Nor was it reasonable to interpret the authorization to protect critical assets as extending to the investigation of a broad set of criminal offenses that could implicate any of the Department's activities. The deputation did not explicitly authorize investigation of criminal offenses or enforcement of criminal laws. Nor did it list specific criminal offenses that were within its purview.

The Department had been on notice of potential issues with the deputation since at least 2017. The OIG at that time concluded that the deputation of ITMS agents as part of the "protection detail" on the deputation appointment form did not clearly establish their authority to investigate criminal offenses. OIG briefed the Department on this issue in July 2017. In an August 2, 2017, letter to USMS, the OIG explained that the Department had "assured" it that the "verbiage on the [special deputation forms] would be revisited and re-coordinated with USMS if necessary" and that the Department "would further research [ITMS]'s authority requirements and limitations." The Review Team did not uncover any evidence that the Department sought to clarify the scope of the deputation with USMS or otherwise address the issue identified by the OIG. To the contrary, the Department continued to seek deputations for ITMS agents as part of the "Protection Detail."

It is not clear that the Office of the General Counsel ever provided a clear interpretation of the scope of ITMS's deputation. The Review Team's ability to address this issue is somewhat

---

[6] The Review Team notes that it reviewed a letter from OSY to the USMS, dated April 18, 2005, that requested a "USMS special deputation for conducting investigations of suspected or alleged criminal violations of federal law involving the safety or security of Commerce assets, operations or personnel." The Review Team found no record of the USMS ever granting ITMS a deputation that broad, and it cannot confirm if that letter was ever sent.

limited because it does not have access to every discussion that may have transpired between ITMS and OGC and certain lawyers who worked on ITMS issues over the years were not available to be interviewed. Nor did the Review Team find evidence that OGC was asked to conduct, or in fact conducted, a legal assessment of whether any specific ITMS investigation was within the scope of the deputation. The Review Team also did not find evidence that OGC ever sought USMS's views on the scope of the deputations.[7]

Necessity of ITMS's Criminal Law Enforcement Authority. The Review Team also sought to assess whether the Department needs the broad criminal law enforcement authority that ITMS claimed. The Review Team concludes that it does not. Threats to the Department's security that reflect potential criminal violations can be addressed by making referrals to and working with the OIG, FBI, or other agencies that have statutory law enforcement authority.

As a threshold matter, the Review Team has identified only two ITMS cases in which criminal charges were brought. The number of criminal charges is not necessarily determinative of whether criminal law enforcement authority is necessary. Criminal law enforcement investigations may serve a valuable purpose even if they are resolved without charges being brought.

Another way to assess the need for criminal law enforcement authority is to consider the rationale set out for it in an April 2005 OSY memo about its investigative authority. That memo claimed criminal investigation authority was needed to "develop and compel information" so that OSY could better mitigate threats, protect the Secretary, and clear cases. The Review Team does not believe that the succeeding fifteen years of experience has justified those rationales.

The Department has means to develop and compel information to mitigate threats without reliance on the criminal investigative authority claimed for ITMS. The Department—by virtue of its status as an employer, an owner of information, an operator of information technology systems, etc.—has authority to collect, compel, review, and analyze information from a variety of sources and use a variety of techniques to investigate security breaches and violations of security policy.

The Review Team has identified few instances in which ITMS engaged in core criminal law enforcement techniques to compel information, such as obtaining or executing a search warrant. The Review Team is aware of only two cases in which a warrant was executed. In both of those cases, other federal law enforcement agencies with statutory authority to seek a warrant participated. An independent ITMS authority to seek a warrant was not essential.

The independent exercise of the criminal law enforcement authority ITMS claimed is not necessary for the Department. In security matters where exercising criminal law enforcement authority may be necessary, the Department can refer matters to agencies with statutory criminal law enforcement responsibility and coordinate with them as appropriate.

---

[7] The conclusions in this report about the USMS deputation apply only to the deputations for ITMS. The Department's Executive Protection Unit (EPU), which provides physical protection to the Secretary, also receives a deputation from the USMS. That unit is distinct from ITMS and does not participate in ITMS's mission. The issues described in this report do not apply to the EPU's deputations.

2. *Administrative Investigations*

Administrative investigations do not rely on criminal law enforcement authority. They rely on other authorities, such as the Department's authorities as an employer or authorities related to the handling of classified information.

While the Review Team has not reviewed all ITMS case files, it appears that most of the investigations conducted by ITMS were administrative in nature, and many of these matters were appropriate for investigation. A number addressed alleged security incidents or violations. Others related to referrals from outside agencies or from the Department's Personnel Security Program of matters that could implicate the suitability of an individual for a security clearance.

The Review Team noted that there did not appear to be a clear line between ITMS's administrative investigative functions and criminal investigative functions. Notably, the 2005 OSY investigative authority memo claimed that because OSY's "security mission is intrinsic to the identification, assessment and management of threats, very few cases would not have an actual or potential criminal character." Many ITMS agents interviewed stated that criminal investigations typically started as administrative.

Criminal law enforcement authority is not necessary to conduct administrative investigations implicating the Department's security. In most, if not all, cases, the Department can conduct administrative investigations and mitigate related security threats without needing to exercise criminal law enforcement powers. For example, in cases involving the mishandling of classified information, the Department may be able to determine how an employee handled information by relying on administrative investigative resources, including the ability to review relevant information on Department IT systems, voluntary interviews with persons involved and, if necessary, interviews that compel employees to answer questions or face potential discipline. The Department can often mitigate such threats without its own criminal law enforcement authority by suspending or terminating an employee's access to classified information, taking other personnel action, or referring matters to appropriate criminal law enforcement authorities.

The Review Team has concluded that a specialized investigative unit is not necessary to conduct administrative investigations. Responsibility for security-related administrative investigations can be vested in preexisting units with relevant subject matter expertise. For example, the Department's information security program, which is responsible for policy and procedures for the protection of classified information, can also have the responsibility for reviewing alleged violations of those policies and procedures.[8]

3. *Protective Intelligence*

The role of protective intelligence is to assess information relevant to potential threats against the Secretary and other designated Department officials. Protective intelligence is part of ITMS's mission. This is distinct from the physical protection of the Secretary. The Department's Executive Protection Unit (EPU), which is separate from ITMS, provides this protection.

The Review Team found that aspects of ITMS's protective intelligence mission are appropriate for mitigating potential threats to the Secretary. For example, the Department should have

[8] *See* Dep't Org. Order 20-6, § 3, *available at* https://osec.doc.gov/opog/dmp/doos/doo20_6.html.

personnel who review potentially threatening correspondence sent to the Secretary and coordinate a response. This could include conducting research on the sender, reaching out to criminal law enforcement authorities for further investigation, and coordinating information sharing between those authorities and the EPU and physical plant security so that any necessary precautions can be taken.

However, certain ITMS practices on protective intelligence—apparently conceived of by ITMS leadership and questioned by some agents—went beyond the appropriate scope for a protective intelligence function and should be discontinued. Specifically, ITMS had a practice of opening protective intelligence intakes on matters where there was no apparent threat to the Secretary or other Department official. It appears that, over many years, ITMS would be sent select correspondence for review, regardless of whether it posed a threat. ITMS would then open an intake in relation to the correspondence, even in the absence of a discernable threat. This process would have an agent complete an intake form, run the names of the author or others associated with the correspondence in various databases in search of any relevant information about the person (often there was none), and then document these activities. No further activity appears to have occurred in the clear majority of these instances. Hundreds of the 1,945 open cases existing at the time of this Review appear to fit this pattern. Several agents interviewed stated that this activity accounted for much of the protective intelligence work of ITMS. EPU reported that it did not receive regular briefing on protective intelligence matters from ITMS and instead sought protective intelligence from other government agencies.

The Department should continue a protective intelligence function, subject to the limits of the Department's legal authority to conduct this work. It should ensure that appropriate policies and procedures governing such activities are in place, accompanied by routine oversight. The Department should define the scope of appropriate protective intelligence matters and assign EPU to carry out this function.

4. Insider Threat Detection

Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," requires federal agencies to "implement an insider threat detection and prevention program consistent with guidance and standards developed by the [National] Insider Threat Task Force."[9] An insider threat program has multiple components. According to the National Insider Threat Policy,

> Critical program requirements include but are not limited to: (1) monitoring user activity on classified computer networks controlled by the Federal Government; (2) evaluation of personnel security information; (3) employee awareness training of the insider threat and employees' reporting responsibilities; and (4) gathering information for a centralized analysis, reporting, and response capability.[10]

---

[9] Exec. Order No. 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information (Oct. 7, 2011).

[10] Presidential Memorandum on National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, Nov. 12, 2012, *available at* https://www.dni.gov/files/NCSC/documents/nittf/National_Insider_Threat_Policy.pdf.

In September 2014, the Department designated OSY and the Office of the Chief Information Officer to implement the Department's Insider Threat Program. OSY was to act as the "hub" to "analyze indicator data and reports provided by covered persons and refer matters of investigative interest to designated entities in accordance with Department regulations for action as appropriate." The "hub" activity became the responsibility of ITMS. ITMS also retained the responsibility to investigate matters emerging from the hub that posed a threat to Department security.

ITMS's insider threat activities are not clearly distinguished from its other investigative activities. Not all other departments combine insider threat detection with criminal or counterintelligence functions. Although there is no uniform model for organizing the insider threat function, the Review Team spoke with agencies that enforce a clear separation between their insider threat "hub" programs and any criminal law enforcement or counterintelligence investigative authorities. These programs provide initial analysis of information about potential risks and then, as necessary, refer matters to authorities with criminal law enforcement or counterintelligence authorities. Referrals could also be to human resources, employee assistance programs, supervisors, or other channels, depending upon the nature of the information. This approach reflects many of the best practices for insider threat program design highlighted by the National Insider Threat Task Force (NITTF).

The Review Team has concluded that the best path forward for the Department to continue this function is to transition the "hub" role out of ITMS and to a new unit with this dedicated responsibility. This new unit should not be responsible for criminal or counterintelligence investigations arising out of the matters it analyzes. Rather, it should develop relationships with appropriate external partners, like the OIG or FBI, for referral of matters when warranted. The Department should consult with NITTF in this effort. This will help ensure that this new unit complies with all best practices on insider threat detection.

5. Counterintelligence Functions

Executive Order 12333, "United States Intelligence Activities," defines "counterintelligence" as "information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities, but not including personnel, physical, document or communications security programs."[11] Counterintelligence is a responsibility of the Intelligence Community, which consists of multiple departments and agencies in the federal government. That executive order provides that the FBI is responsible for conducting counterintelligence and coordinating counterintelligence activities within the United States. Neither the Department nor ITMS are members of the Intelligence Community.

Concerns have been raised that ITMS has engaged in counterintelligence without proper authority. This stems in part from how the Department has described ITMS's mission and how ITMS conceived its mission. Department Administrative Order 207-1 states that ITMS is responsible for "conducting counterintelligence investigations involving personnel (e.g., foreign

[11] Exec. Order No. 12333, United States Intelligence Activities (Dec. 4, 1981).

national visitors)." In addition, ITMS categorizes many of its cases as "counterintelligence" or "counterespionage."

The Review Team has not been fully able to assess ITMS's purported counterintelligence mission, as it has not completed review of the substantial volume of classified information at ITMS. The review of that information will continue as part of the closure of ITMS. From what the Review Team has considered so far, it can make the following observations.

First, ITMS sometimes ran names through classified databases to learn about an individual's background. The Review Team did not find any ITMS procedures establishing standards for engaging in this activity. Many ITMS agents expressed concern to the Review Team about this practice.

Second, ITMS had interactions with members of the Intelligence Community. The Review Team is aware of instances in which the Intelligence Community referred matters to ITMS. These matters related to information potentially impacting the suitability of individuals for access to classified information or sensitive Department programs.

Third, the Department has previously claimed that ITMS's counterintelligence role is overstated. In response to an inquiry from the OIG, the Department in May 2019 explained in response that "ITMS did not engage in a dedicated counterintelligence program, does not originate investigative activities solely with the intent of engaging in counterintelligence, and does not engage unilaterally in traditional U.S. Intelligence Community (USIC) counterintelligence operations." A former DAS-IS, who served in the Department in the latter half of 2020, agreed that ITMS used the term counterintelligence incorrectly and that its work was not the kind of counterintelligence work performed by the Intelligence Community. There is evidence that ITMS used the term counterintelligence to describe activities that did not rely on counterintelligence authority. For example, ITMS appears to have used the term to refer to vetting of foreign nationals for access to Department facilities or other matters more correctly identified as insider threat detection.

Fourth, the use of the term counterintelligence raises potential issues. The collection of information in counterintelligence operations rests on different legal authorities, with different legal protections, than the collection of information used for domestic law enforcement or administrative actions. Claiming a counterintelligence mission may have implied that ITMS collected information through counterintelligence means without proper authorization or for non-counterintelligence purposes, either of which could raise serious legal issues. The Review Team has thus far found no evidence that ITMS engaged in such activity but understands why use of the term would cause concern.

The Department should amend the orders and policies regarding ITMS functions to eliminate any implication that the Department's internal security function engages in counterintelligence operations. The Department should also assess the extent to which remaining security functions, *e.g.,* foreign visitor vetting, require access to classified databases and ensure that any continued use of such databases is subject to policies and procedures that comply with all applicable laws.

B. ITMS Policies, Procedures & Training

1. Policies & Procedures

The execution of investigatory authority, especially criminal investigatory authority, requires comprehensive written policies and procedures, vetted by counsel, and approved by management. These should be easy to read and readily available for agents to access when they have a question on what to do in a given situation. These documents should also be regularly reviewed with updates addressing changes in law, best practices, or investigative techniques. Finally, these policies and procedures should facilitate oversight by providing standards for accountability.

The Review Team found that ITMS lacked adequate policies and procedures. While there were some policies and procedures for some ITMS activities, other required policies and procedures were in draft form or do not appear to exist at all. For example, multiple agents told the Review Team that ITMS had no policy on when and how to provide appropriate legal warnings for employee interviews, an issue addressed in the OIG ROI. The OIG ROI also noted that ITMS agents flew armed without a required flying-armed policy, in violation of Transportation Security Administration requirements. Multiple agents told the Review Team that they only received one or two formal policies for review and signature—a use of force policy and a weapons qualification policy. One agent contrasted this to a previous law enforcement job in which an initial binder of policies and periodic policy updates were distributed for agents to review and sign.

The Review Team documents some of the key observations about ITMS policies and procedures below.

Case Files, Evidence & Classified Material. Consistent handling of case files and evidence is essential for an investigatory unit. It helps ensure complete and accurate records are available to take action when warranted and defend that action in court.

ITMS did not have effective practices for maintaining case files and evidence. The Review Team was not able to locate an adequate written policy or guide for organizing or preserving investigative files. Agents interviewed generally agreed that ITMS's practices in this area were deficient. The Review Team observed many reasons for this deficiency.

First, ITMS's central case management tracking system was not up-to-date and was incomplete. ITMS tracks its cases in a classified Microsoft Excel spreadsheet. Some agents interviewed stated that this spreadsheet lacked proper version control and was not consistently updated. There are some instances in which there is little or no information beyond a case number in the tracking spreadsheet.

Second, ITMS's digital files are not consistently maintained. ITMS maintains its files in a digital system called CNET. Agents interviewed stated that there are cases listed in the case tracking spreadsheet without corresponding information on CNET.

Third, ITMS's physical files are not organized. The OIG ROI observed that one portion of ITMS office space included a law enforcement badge and credentials that were not properly accounted for among "piles of disorganized and haphazardly-placed papers, notebooks, and media." The Review Team observed a similar lack of organization in various ITMS workspaces.

Fourth, ITMS did not have adequate standards for maintaining evidence. ITMS would not promptly log all evidence. In some cases, it would collect evidence but never review it. Although the Review Team found an evidence policy dated November 2016, multiple agents told the Review Team that they did not know if ITMS had an evidence policy and they had not been provided one. The Review Team noticed a number of irregularities in a sample of evidence processing forms it reviewed: five of nine forms did not list a case number, there seemed to be a delay in receiving evidence and entering it in to the evidence vault, forms related to email searches did not list a subject or associated email account, and some forms stated that the purpose for the collection was "safe keeping," which is outside of the Review Team's experience as a reason to enter and store evidence.

Fifth, ITMS did not always properly control classified information. As documented in the OIG ROI, there was evidence of a practice in ITMS of failing to document the transfers of classified documents in accordance with Department policy. As part of certain curative efforts undertaken in the fall of 2020, work was done to inventory classified documents and locate material not properly accounted for.

Reconstructing and archiving ITMS records, to the extent practicable, is important. The Review Team initiated a project to identify all records found within several office spaces and organize them in a proper record-keeping system. This work began over the summer 2021 and remains ongoing as of the date of this report.

Closing Cases. A proper investigative function has periodic case reviews and closes cases when action is no longer warranted. ITMS does not have an effective practice for reviewing cases for closure and closing those that did not need to remain open.

When this Review began, ITMS had approximately 1,945 cases. The vast majority, if not all, of those cases should have been closed, in some cases months or years before the Review began. The Review Team estimates that as many as 85% to 90% of the open cases have had no activity since before January 1, 2020. This prolonged inaction indicates that a case either lacks further leads worth pursuing or is not a priority.

The Review Team also notes that continued activity in many ITMS cases may not have been warranted. Some agents interviewed said that the ITMS Director would sometimes reassign an inactive matter to a new agent, and that that new agent would repeat investigative steps the prior agent had taken. While circumstances sometimes warrant a fresh set of eyes, nothing in the case files the Review Team examined justified the second look. The Review Team cannot say how often this duplication of effort occurred, but it has reviewed several case files that show this pattern.

ITMS should not have had so many open cases. A process began in the fall of 2020 to close cases, and certain ITMS agents at that time worked to prepare cases for closure. For unclear reasons, that process stalled without the closure of cases. The Review Team has resumed a process for reviewing open cases and directing their closure. That process remains ongoing.

Email Searches. The Department can search employee work emails without a warrant because employees do not have an expectation of privacy in their work emails. Even though a warrant is not required, a proper policy on email searches would outline the circumstances in which a search is appropriate, guidelines on defining the scope of the search, the process for obtaining

supervisor approval for the request, and direction on how to forensically review and preserve the evidence collected by the search. This would also establish a clear written record for the reason for the search, the scope of the search, and the dates and persons involved in the request. This facilitates the use of the evidence obtained in the search if the Department needs to act on the evidence by establishing a clear chain of custody and a clear documentation of the purpose of the search. It is also essential to conducting oversight.

ITMS practice on email searches did not meet these standards.

ITMS would request emails from Department and bureau IT officials. It is not clear that ITMS had any standard for determining when to make these requests. ITMS also did not consistently document its search requests in writing. Sometimes it did, but sometimes it made requests over the phone or in person. As a result, documentation of the scope and purpose of the email search was not systematically kept. Because of the inconsistent documentation practices, it is not possible for the Review Team to obtain a precise count of the number of times ITMS sought employee emails.

The lack of adequate documentation creates problems for accountability. As noted in the OIG ROI, there were instances in which the OIG could not confirm whether or why emails had been searched because of the limitations on records. In one such instance, it was alleged that emails may have been pulled to review correspondence between an employee and OIG. That could raise concerns of retaliation if someone were seeking to monitor communications with the OIG. However, the OIG could not ascertain the motivation for the email request. Multiple ITMS agents expressed a similar concern that their supervisors would review their own emails for inappropriate purposes. Following clear standards for requesting and documenting email searches could have mitigated these issues.

2. Training

Training is an essential component for an investigatory unit. This includes basic training that is a requirement for employment in the unit, formalized training that is specific to the mission of the unit, and continuing education to ensure agents stay up to date on best practices. Given ITMS's mission, the Review Team would expect specialized criminal investigation, counterintelligence, protective intelligence, and insider threat training to be part of an appropriate training program.

The Review Team assessed ITMS's training documents, reviewed information on prior training of ITMS agents, and asked ITMS agents about the trainings they have received, both from ITMS and from other sources. The Review Team concludes that ITMS training requirements were not adequate for its mission.

Minimum Training Requirement. The criminal investigator job series that ITMS agents hold requires basic criminal investigation training. The federal law enforcement community generally considers the accredited Criminal Investigator Training Program (CITP) conducted by the Federal Law Enforcement Training Center (FLETC), or an equivalent course, as appropriate training for the criminal investigator job series.

The Review Team found that ITMS did not have a standard practice for ensuring that its agents received CITP or equivalent training. Only six of the 11 current ITMS agents have completed CITP. Based on standard federal law enforcement practice, ITMS would have to determine that

the remaining five attended CITP equivalent courses (or would have to send them to CITP). The Review Team did not find any written standards by which ITMS would determine that alternative training was the equivalent of CITP. The Review Team does not believe that this determination could have been made for ITMS's two longest tenured agents, including the ITMS Director. Those agents have completed only FLETC's Mixed Basic Police Training Program (now known as the Uniformed Police Training Program). Mixed Basic is a basic law enforcement program intended for uniform police officers. It is not the specialized investigative training that CITP offers.

Mission Specific Training. The only required mission-specific training for ITMS agents that the Review Team found was "Basic Agent Training" (BAT). The ITMS Director created BAT. The most recent BAT took place in the Shenandoah Mountains over a two-week period and included training on surveillance, investigation, and less than lethal uses of force. Many agents failed the training, but, at least after the most recent BAT, no remedial training was required.

The Review Team does not believe that the BAT was appropriate training. First, multiple agents interviewed reported that BAT did not adequately prepare them for ITMS's mission. Second, the Review Team found no evidence that the creator and presenter of the training had attended the FLETC accredited program for law enforcement instructor training or any comparable course. Third, the BAT was not accredited. Accreditation is an important reflection of adequacy, as explained by the Federal Law Enforcement Training Accreditation (FLETA) program: "accreditation of a federal law enforcement academy or training program demonstrates to the citizens they serve that the training organization has voluntarily submitted to a process of self-regulation and successfully achieved compliance with a set of standards that has been collectively established by their peers within their professional community."[12] The Review Team did not find any evidence that ITMS sought accreditation for the BAT or otherwise sought an independent assessment of its adequacy.

C. Oversight

1. Direct ITMS Management & Oversight

The Review Team concludes that, at least for the last several years, the Department exercised inadequate management and supervision over ITMS's activities. Although some efforts at increased oversight occurred, it does not appear that the Department appreciated the need for enhanced comprehensive and coordinated management of ITMS.

There were a number of instances in recent years that indicated ITMS needed greater oversight:

- In 2016, ITMS began an investigation into the Office of Executive Support (OES), which was responsible for providing intelligence support in the Department, including receiving and handling classified information and briefing the Secretary on intelligence matters. This investigation lasted for four years. Some in management tried to get ITMS to resolve the case sooner, but without success. While the Review suggests the investigation was warranted at the outset, there was no apparent basis for its duration. A result of this

[12] *Federal Law Enforcement Training Accreditation History*, Federal Law Enforcement Training Accreditation, Sept. 2, 2021, *available at* https://www.fleta.gov/site-page/history.

prolonged investigation was that many OES employees were paid without being put on leave and without be given alternative work for a long period of time.

- Management was also on notice of issues through the work of the OIG, in particular the OIG's questioning of ITMS's deputation and counterintelligence authorities in 2017 and 2018, respectively, as described above. On the deputation issue, there was no evidence that management sought to clarify the scope of the USMS deputation issue with the USMS at that time. On the counterintelligence issue, the Department agreed that it would remove counterintelligence from the description of ITMS's mission but it never did so.
- ITMS suffered from chronic personnel attrition, losing on average 25% of its staff each year since 2010.
- In 2019 and 2020, management also allowed ITMS to intervene in the Census Bureau's efforts to maintain network security and combat disinformation without a clear justification for ITMS's involvement. The Census Bureau already had a team of professionals working on these issues and was collaborating with other government agencies with relevant authorities and expertise before ITMS got involved. From what the Review Team has seen, ITMS did not bring any new skill sets to these efforts. ITMS's activities were ultimately curtailed in the latter half of 2020 by an appointee who joined the Department in 2020.

More broadly, the Department did not ensure adequate training for ITMS agents, including the most important senior leadership position in ITMS. Given the complexity of ITMS's mission, the Department should have required rigorous, accredited, and regular training. It did not.

The Review Team did not find adequate mechanisms in place to ensure accountability. For example, performance metrics can be a key to oversight. Several performance metrics could be useful in overseeing an investigative unit, including case closure rates, the average time necessary to complete an investigation, the number of cases in which allegations are substantiated, the number of remedial actions generated from investigations, and more. The Review Team found no evidence that management adequately assessed ITMS along these or other appropriate metrics. This is perhaps one reason why ITMS could maintain so many open cases for so long.

Routine compliance inspections are another form of accountability. The Office of Export Enforcement, for example, submits its field offices to internal compliance audits on a specified schedule. ITMS, however, was not subject to regular compliance inspections. OSY has a Plans, Programs, and Compliance Division, but the Review Team found no indication that OSY has tasked this Division with reviewing ITMS. Such a review may have addressed some of the deficiencies noted in this report.

The Department permitted ITMS's excessive use of non-disclosure agreements (NDAs). In some instances, ITMS even required its own supervisors, lawyers and other senior leaders to sign NDAs. Although an NDA may be appropriate in some cases, ITMS's widespread use of NDAs appears unnecessary because government employees already have obligations to limit the disclosure of sensitive information. These NDAs contributed to a culture where supervisors felt unable to communicate with each other over issues relevant to their office and supervision. Additionally, no policy explaining the purpose, limitations, and use of NDAs was found. The Review Team could not determine why the Department permitted this practice.

Furthermore, there does not appear to have been adequate scrutiny of ITMS's budget or spending. ITMS's case load does not appear to justify the number of full-time employees that it sought. It is also not clear that OSY management was adequately scrutinizing ITMS's purchases, which included surveillance and other equipment not justified for its mission.

2. Legal Oversight

An investigative unit requires a close working relationship with legal counsel. That is particularly true for ITMS. Criminal law enforcement, administrative investigations, insider threat detection, and counterintelligence are each governed by different legal regimes. Each activity can regularly raise questions of legal authority, privacy, civil rights and civil liberties. Any one of these activities would require close legal coordination and supervision. The fact that ITMS sought to engage in so many legally complex activities heightened the need for regular and rigorous legal advice.

The Review Team found that ITMS did not have a sufficiently integrated relationship with OGC. Attorneys in OGC did make efforts to resolve issues related to the OES investigation and advocated for the reorganization of the Department's intelligence and security functions as means to improve oversight. But ITMS did not have its own counsel, or an attorney in OGC specifically assigned to provide legal support to ITMS (except for a brief period in the latter half of 2020). OGC provided ITMS with legal advice on an as-requested basis when ITMS raised legal questions. These questions were addressed by a variety of different lawyers over time. The Review Team could not determine the extent to which these OGC attorneys communicated with each other or whether any lawyer in OGC had sufficient information about the breadth of ITMS's work to fully assess and advise those in the Department with management responsibility for ITMS of the legal risk ITMS's activities posed to the Department.

OGC was aware of ITMS's practice of requiring senior leadership to sign NDAs. Indeed, ITMS required several OGC attorneys to sign such NDAs. The Review Team found no evidence that any OGC attorney sought to curtail this practice or to advise other Department officials the potential impediment widespread use of such NDAs could pose to effective oversight of ITMS.

OGC also knew that ITMS engaged in employee office searches. It is not clear that OGC asked to see the search operations plans that ITMS had developed for these searches or was fully aware of the tactics ITMS employed in conducting the searches. OGC appears to have been consulted about some of the email searches, but the Review Team found no evidence that ITMS reliably sought OGC's advice.

Going forward, OGC should dedicate legal resources to provide regular and proactive advice for the administrative investigation, protective intelligence investigation, and insider threat detection activities that will continue.

3. Additional Factors Contributing to Inadequate Oversight

ITMS's claim to criminal law enforcement and counterintelligence missions may have impacted Department oversight. From the perspective of Department employees, ITMS operated from a position of presumed authority to investigate matters that had a bearing on criminal law enforcement, counterintelligence, or national security. Many facts contributed to this appearance, including: the overbroad description of ITMS authorities in Department orders, the fact that the

ITMS agents were criminal investigators who carried and displayed law enforcement badges, the routine insistence on the signing of NDAs, and ITMS's contacts with other law enforcement agencies. It was apparent to the Review Team that employees were reluctant to question officials who claimed and displayed the attributes of criminal law enforcement and counterintelligence authority. That may have been especially true for the majority of Department employees who do not have criminal law enforcement or counterintelligence experience. The Review Team believes that this dynamic contributed to excessive deference and inadequate oversight.

D. Allegations of Racial and Ethnic Profiling

As the Department of Justice has explained, race, ethnicity, national origin, and other protected characteristics "should never be the sole basis for a law enforcement action."[13] Practices that rely on bias "are unfair, promote mistrust of law enforcement, and perpetuate negative and harmful stereotypes."[14] Accordingly, Department of Justice guidance provides that "Federal law enforcement officers may consider race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity only to the extent that there is trustworthy information, relevant to the locality or time frame, that links persons possessing a particular listed characteristic to an identified criminal incident, scheme, or organization, a threat to national or homeland security, a violation of Federal immigration law, or an authorized intelligence activity."[15]

It has been alleged that ITMS opened, prolonged, and refused to close cases based on race, ethnicity, or national origin. Without diminishing the seriousness of these allegations, the Review Team observed that prolonging cases and failing to close them appear to have been systemic issues with ITMS, as described above. The Review Team also reviewed specific cases in which discrimination has been alleged.[16] The Review Team reviewed case files and interviewed some of the agents involved (in other cases, agents involved are no longer with the Department and declined to be interviewed). The Review Team has not found any firsthand or documentary evidence that racial, ethnic, or national origin bias motivated any specific cases.

It has also been reported that ITMS engaged in broad searches of Department of Commerce servers for particular phrases and words in Mandarin as part of talent recruitment investigations. The Review Team confirmed that allegation. According to information the Review Team was able to uncover to date, it appeared that ITMS ran this search several times, with the last documented time being March 2018. Because of the state of ITMS records, the Review Team cannot confirm every instance in which these searches were run.

According to the FBI, the talent recruitment programs of the People's Republic of China target "scientists, engineers, professionals, foreign government employees, and contractors to bring

---

[13] *Guidance for Federal Law Enforcement Agencies Regarding the Use of Race, Ethnicity, Gender, National Origin, Religion, Sexual Orientation, or Gender Identity*, Department of Justice (Dec. 2014), *available at* https://www.dhs.gov/sites/default/files/publications/use-of-race-policy_0.pdf.

[14] *Id.*

[15] *Id.*

[16] The Review Team also is aware of allegations of unlawful employment practices against ITMS employees. Employment discrimination allegations are beyond the scope of the review, and many had already been addressed through relevant human resources or EEO channels.

foreign research and technology with them to Chinese universities, businesses, and state-owned enterprises in China."[17] Depending on the circumstances, federal employee participation in a talent recruitment program for compensation can violate criminal laws prohibiting employees from receiving outside compensation for their government work and can raise concerns about the inappropriate disclosure of sensitive information.

In furtherance of a talent recruitment investigation, ITMS went to the offices of the Chief Information Officer in at least certain Department bureaus with a list of search terms and requested that those search terms be run across the bureau servers. The search terms included phrases in Mandarin. The focus of the talent recruitment investigation was China and these search terms appear to have been generated, at least in part, by prior talent recruitment cases and in reference to known talent recruitment programs. Some of the search terms were specific and referred to the names of these programs. Some were generic terms, like the word "thousand," which appeared in the name of a supposed talent recruitment program but was isolated out as a single word for searching. The Review Team confirmed that these searches were done on National Oceanic and Atmospheric Administration, National Institute of Standards and Technology, United States Census Bureau and United States Patent and Trademark Office servers at the request of ITMS officials. The Review Team did not find clear evidence of why these bureaus were chosen and was not able to confirm every bureau that may have been asked to conduct these broad searches due to incomplete recordkeeping practices. As these searches were conducted bureau-wide, it does not appear that particular employees were targeted in these broad searches. ITMS also tried to identify individuals associated with these programs by conducting open-source internet searches. These searches would use terms associated with the talent recruitment programs and the names of the Department's bureaus. At least some of these open-source searches appeared to cover all the Department's bureaus, not just NOAA or NIST. Finally, the Review Team did not find evidence that ITMS searched for specific ethnic surnames, which has been alleged.

The results of the searches were subsequently provided to the OIG, which assumed responsibility for investigating cases based upon fraud and other relevant offenses within the OIG's jurisdiction. OIG also previously received a complaint that ITMS's talent recruitment investigations targeted persons of specific ancestry. In response to that complaint, OIG stated that the "OIG agents working on these cases have observed no reason to believe racial, ethnic, or cultural bias is a motivator in these cases" and deemed the allegation "unsubstantiated."

These broad searches do not, in and of themselves, appear to violate the Department of Justice guidance cited above. Nonetheless, they are understandably viewed with suspicion by employees, oversight authorities, and those outside the Department given the absence of adequate policies, procedures, and oversight governing ITMS activities. The Department should not engage in any future use of these techniques without strict oversight and clear documentation of the rationale.

In sum, the Review Team did not find clear evidence that ITMS pursued any particular investigations based on improper considerations. That said, the Review Team recognizes that it

---

[17] *China: The Risk to Corporate America*, Federal Bureau of Investigation (May 2019), *available at* https://www fbi.gov/file-repository/china-risk-to-corporate-america-2019.pdf/view.

is hard to reassure employees and other stakeholders on this point because of the other findings in this Review regarding ITMS's lack of authority; inadequate policies, procedures, and training; deficient records management and documentation; and inadequate management and oversight.

Discontinuing ITMS's criminal law enforcement and counterintelligence missions may partially address the legitimate concerns of employees and stakeholders. The Department should take additional steps to ensure that its administrative investigations and insider threat detection activities comply with the law and adequately protect civil rights, civil liberties, and privacy. In the next section, the Review Team makes recommendations for improvements to policies and procedures, training, and oversight that can help ensure this occurs.

IV. Recommendations

The Review's comprehensive recommendations for addressing the programmatic and systematic issues raised in the Review and the OIG ROI are set forth below. The Review Team estimates that the wind down of ITMS can be accomplished within approximately 90 days of this report, and that the remaining recommendations can be implemented within 180 days of this report, though many can and will be accomplished sooner than that.

Recommendation #1: The Department should eliminate ITMS, discontinue the criminal law enforcement function that was part of ITMS's mission, clarify that the Department does not possess the authority to conduct counterintelligence activities, and redistribute other remaining functions of ITMS to other offices. This should include:

A. discontinuing any independent criminal law enforcement and counterintelligence functions that ITMS performed;
B. transferring responsibility for protective intelligence for the Secretary to the Executive Protection Unit;
C. transferring any remaining ITMS functions to other units that have existing expertise and capacity or can quickly stand up the expertise and capacity to perform those functions (e.g., investigations of mishandling of classified information should be clearly assigned to the Information Security Division);
D. partnering with the National Insider Threat Task Force to reestablish a more effective and accountable insider threat program within the Office of Intelligence & Security (OIS);
E. designating an appropriate office or offices in OIS for coordinating with and assisting criminal law enforcement or intelligence agencies on an as needed basis;
F. setting forth in policy the legal source of the Department's authorities to conduct the retained functions and the precise scope of the authorized activities;
G. working with the U.S. Marshals Service to clarify, in writing, the scope of the deputations provided to members of the Executive Protection Unit for activities related to the protection of the Secretary;
H. identifying what classified or other databases, if any, the Department should continue to use for the retained functions and ensuring there are adequate policies and procedures governing the use of those databases;
I. ensuring that the Office of the General Counsel designate one or more attorneys responsible for providing legal advice to administrative investigation, protective intelligence, and insider threat functions;

J. preparing the necessary Department budgetary and administrative tasks to accomplish this reorganization; and
K. providing adequate resources to accomplish the recommendations set forth in this Report.

Recommendation #2: The Deputy Assistant Secretary for Intelligence & Security should establish an oversight framework for the office's security administrative investigations and insider threat activities that includes:

A. defining and tracking key performance indicators and metrics that will enable effective managerial and budgetary oversight;
B. establishing standards for when and how matters that require law enforcement or Intelligence Community engagement can be transferred to agencies with the relevant authority and expertise;
C. for those administrative investigations of security violations that remain the Department's responsibility, requiring periodic reviews of all open administrative investigations;
D. establishing a regular cadence for compliance reviews by the Plans, Programs, and Compliance Division of OSY;
E. developing training requirements for administrative investigations and insider threat personnel that comply with best practices;
F. convening a security and insider threat review board at least semiannually with members from the Office of the Deputy Secretary, the Office of the General Counsel, the Office of Civil Rights, and other Departmental units as appropriate, to review the performance, policies, and priorities of the Department's security investigations and insider threat functions; and
G. in the short-term, the Deputy Assistant Secretary for Intelligence & Security should consult with the FBI, the OIG, and any other relevant agencies to develop processes for transfer of any open ITMS investigations that require further action.

Recommendation #3: The Deputy Assistant Secretary for Intelligence & Security, in conjunction with the Office of the General Counsel, should develop written policies for the office's administrative investigations and insider threat functions that comply with all applicable laws and ensure that adequate safeguards exist to protect civil rights and civil liberties. This should include:

A. working with other Department stakeholders to help establish Departmental guidelines, approval paths (including legal review), and documentation requirements, for conducting employee searches, including office searches and email searches, for security purposes;
B. ensuring that all data is collected, retained, and destroyed in accordance with applicable laws and regulations;
C. working with the Department's Office of Privacy and Open Government to ensure that appropriate Privacy Act systems of records are established;
D. working the with Department's Records Officer to ensure
    a. appropriate records retention schedules are developed; and
    b. all staff receive appropriate training on records procedures; and
E. requiring regular training for investigatory and insider threat personnel on civil rights, civil liberties, privacy and data collection, implicit bias, and related issues.

Recommendation #4: The Deputy Assistant Secretary for Intelligence & Security should continue the ongoing work to close and archive ITMS cases, establish an appropriate schedule for the destruction of this information that complies with applicable law, and implement policies to ensure that no information developed by ITMS records informs future decisions without a prior legal review and independent factual corroboration. This process should include:

A. completing the processes to close ITMS cases and collect, organize, and archive files and case materials;
B. reviewing any ITMS cases that led to an adverse employment action to determine whether there was any potential misconduct that should be referred to the OIG or other appropriate authority;
C. responding to Privacy Act and FOIA requests from Department employees seeking information on whether they were the subject of an ITMS case and communicate realistic timelines to these employees on when they can expect a response; and
D. placing a statement in ITMS investigatory files alerting the reader that no information in that file developed by ITMS should be the basis of any adverse action without prior legal review and independent verification of the information.

As noted above, the Department has also taken personnel actions in connection with the findings of misconduct in the OIG ROI. The Review Team has also provided information to management to inform decisions. The Review Team has also provided information to the OIG in connection with the investigation of other potential misconduct. The Department will continue to provide information and cooperate with the OIG on all such matters.