U.S. SENATE COMMITTEE ON
COMMERCE, SCIENCE, & TRANSPORTATION

COMMITTEE INVESTIGATION REPORT

ABUSE AND MISCONDUCT AT THE COMMERCE DEPARTMENT

JULY 2021

Prepared by Commerce Committee Minority Staff

Table of Contents

I. EXECUTIVE SUMMARY

In early February 2021, U.S. Senate Commerce, Science, and Transportation Committee Minority Staff launched an investigation into alleged misconduct in the Investigations and Threat Management Service (ITMS) at the Department of Commerce. The investigation began after whistleblowers reported a variety of improper activities dating back to the mid-2000s involving abuses of authority, mismanagement, and reprisal against Department employees. Minority Staff conducted over 100 interviews and reviewed thousands of documents supporting allegations from over two dozen whistleblowers.

The Department of Commerce established the ITMS to provide security services to the Secretary during the George W. Bush administration. Soon after it was established, the unit began performing a law enforcement mission. Under the Obama administration, the ITMS began regularly conducting criminal investigations related to threats against the Secretary and departmental assets, and eventually began using counterintelligence tools to gather information about both foreign visitors and U.S. citizens. The unit continued these activities until early in the Biden administration, despite lacking proper authorization to perform law enforcement functions on behalf of the Commerce Department.

Investigations launched by the unit often lacked a sufficient basis. Although many investigations targeted legitimate threats, the ITMS appears to have opened cases on a variety of employees for the purpose of exaggerating the unit's ability to uncover security risks within the civil service. The unit targeted visible employees across the Department, including award-winning professionals whose background investigations had been successfully adjudicated by other agencies. These probes often resulted in suspended or revoked security clearances, although subsequent reviews largely determined that the unit's allegations lacked merit. The ITMS also broadly targeted departmental divisions with comparably high proportions of Asian-American employees, ostensibly to counter attempts of espionage by individuals with Chinese ancestry. Former and current ITMS employees became subjects as well for challenging the lawfulness of the unit's practices.

Poor management and weak oversight allowed the ITMS to operate outside the norms of the law enforcement community. Deficient policies and procedures outlining the unit's investigative capabilities led to repeated instances of malfeasance, including the purposeful prolonging of investigations, unauthorized use of secured messaging systems, and overclassification of documents to protect the unit from external scrutiny.

The Office of Inspector General Peggy Gustafson (OIG) reviewed multiple complaints of misconduct and abuse related to the ITMS beginning in 2017. Despite clear and convincing evidence, the Inspector General failed to identify and address the unit's deficiency of law enforcement authority and did not satisfactorily act upon the finding that the ITMS collaborated with the Intelligence Community. Although the Inspector General's limited disclosures to Minority Staff reveal that the office investigated many of the unit's unlawful practices, OIG officials made no significant findings.

II. TABLE OF ACRONYMS

Entity	Abbreviations
Basic Agent Training	BAT
Bureau of Industry and Security	BIS
Central Intelligence Agency	CIA
Criminal Investigator Training Program	CITP
Computer Network	CNET
Department Administrative Order	DAO
Department of Homeland Security	DHS
Department Organization Order	DOO
Department of Commerce	DOC
Federal Bureau of Investigation	FBI
Federal Law Enforcement Training Center	FLETC
Freedom of Information Act	FOIA
Federal Protective Service	FPS
Immigration and Customs Enforcement	ICE
Investigations and Threat Management Service	ITMS
Joint Worldwide Intelligence Communications System	JWICS
Mixed Basic Police Training Program	MBPTP
Memorandum for the Record	MFR
National Crime Information Center	NCIC
National Counterintelligence and Security Center	NCSC
National Oceanic and Atmospheric Association	NOAA
National Security Agency	NSA
Office of the Director of National Intelligence	ODNI
Office of Executive Support	OES
Office of the Inspector General	OIG
Office of Personnel Management	OPM
Office of Security	OSY
Operations Security	OPSEC
Personal Identity Verification	PIV
Protective Service Operations Training Program	PSOTP
Salaries and Expense appropriation	S&E
Special Agent in Charge	SAC
Sensitive Compartmented Information Facility	SCIF
Targeted Violence Information Sharing System	TAVISS
Uniformed Police Training Program	UPTP
United States Marshals Service	USMS
Working Capital Fund	WCF

III. FINDINGS

- Investigating threats against the Secretary of Commerce and the Department's assets without a clearly defined mission ultimately led to the mutation of the ITMS into a rogue, unaccountable police force across multiple presidential administrations.

- Since the ITMS lacks statutory police powers, it depended on a delegation of law enforcement authority to agents through the U.S. Marshals Service for the purpose of providing protection to the Secretary and the Department's "critical assets." Although the ITMS originally provided only protective services, the undefined meaning of "critical asset" allowed the unit to engage in a variety of improper law enforcement activities.

- Conducting criminal investigations led to chronic abuse of the Special Deputation program. ITMS agents engaged in law enforcement activities outside the scope of the delegated authority from the U.S. Marshals Service.

- The Special Deputation program lacks sufficient oversight from the U.S. Marshals Service.

- Federal prosecutors regularly dismissed criminal referrals from the ITMS based on identifiable flaws in methods the unit relied upon to obtain evidence. Successful prosecutions of cases investigated by ITMS are few in number.

- The ITMS collaborated with agencies in the Intelligence Community to conduct counterintelligence operations, despite lacking any form of legal authorization to participate in these activities.

- ITMS investigations resulted in covert searches involving identity-concealing tactics, including the use of facemasks, latex gloves, and shoe coverings. The unit also seized work phones and computers to perform digital content searches, and picked the locks of offices and personal storage containers.

- Poor management and weak oversight allowed the ITMS to operate outside the norms of the law enforcement community. Deficient policies and procedures outlining the unit's investigative capabilities led to repeated instances of malfeasance, including the purposeful prolonging of investigations, unauthorized use of secured messaging systems, and overclassification of documents to protect the unit from outside scrutiny.

- Overclassification allowed the unit to block the release of investigative files for criminal targets whose cases proceeded through the judicial system and to members of the public requesting documents through the Freedom of Information Act.

- The ITMS targeted former and current employees for challenging the lawfulness of the unit's practices, demonstrating an egregious pattern of reprisal.

- Across the Department of Commerce, the ITMS opened frivolous investigations on a variety of employees without probable cause for the purpose of exaggerating the unit's ability to uncover security threats within the civil service.

- The ITMS searched Department servers and monitored employee email accounts to scan for evidence of foreign influence as early as 2014. These searches began focusing on an operation to uncover connections between Department employees and actors within the Chinese government. To achieve this end, the ITMS targeted departmental divisions with comparably high proportions of Asian-American employees.

- The Department of Commerce used the Working Capital Fund to fund the ITMS with the resources it needed to conduct investigations largely out of sight from the congressional appropriations process. This allowed the unit to operate with minimal accountability and sustain a mission irreconcilable with its intended purpose of providing protective security services.

- Past investigations into the ITMS from the Inspector General at the Department of Commerce lacked the veracity to identify and resolve the unlawful conduct that has plagued the unit for more than a decade.

- Because of inadequate oversight by the Inspector General's office, the unit's improper exercises of law enforcement powers likely resulted in preventable violations of civil liberties and other constitutional rights, as well as a gross abuse of taxpayer funds.

IV. INTRODUCTION

President Theodore Roosevelt signed legislation that created the Department of Commerce in 1903. The Department currently has approximately 47,000 employees in twelve bureaus in all fifty states and around the world.[1] The missions of the department include promoting economic development and security, enforcing trade agreements, compiling information on the U.S. economy and population, and managing the nation's oceanic resources.[2]

In addition, the Department of Commerce protects national security by safeguarding commercial interests against illegal trade practices, intellectual property theft, and cybercrime.[3] As the Annual Threat Assessment of the U.S. Intelligence Community concluded, China poses a serious threat to the United States in these areas.[4] The report noted that "China will continue expanding its global intelligence footprint to better support its growing political, economic, and security interests around the world."[5] In particular, "China will remain the top threat to U.S. technological competitiveness as the [Chinese Communist Party] targets key technology sectors and proprietary commercial and military technology from U.S. and allied companies and research institutions associated with defense, energy, finance, and other sectors."[6]

Espionage has emerged as a primary tool used by the Chinese government to advance its technological capabilities.[7] Safeguarding key interests against this threat to U.S. security, however, does not absolve any department in the federal government from operating within the bounds of the law. While pursuing security threats, both foreign and domestic, is of paramount importance, federal officials must always base their investigations and law enforcement efforts on the constitutional principles of probable cause and due process. For more than a decade, the Investigations and Threat Management Service (ITMS), which is tasked with conducting investigations to identify and assess critical threats to the Department's mission, operations, and personnel, has failed to uphold this standard.

The ITMS lacks statutory police powers. Instead, the U.S. Marshals Service offers a delegation of law enforcement authority to agents through the Special Deputation program for the purpose of providing protection to the Secretary and the Department's "critical assets." Over a period of sixteen years, the ITMS has abused this program by exercising the delegated law enforcement power to pursue criminal matters. The Commerce Department even eventually began describing the ITMS as a body that "fulfills U.S. national strategic requirements involving counterintelligence, transnational crime, and counterterrorism" by investigating "serious threats to national security" as well.[8] Despite performing functions in collaboration with the Intelligence

---

[1] DEP'T OF COMMERCE, HISTORY, *available at*, https://www.commerce.gov/about/history.
[2] DEP'T OF COMMERCE, ABOUT COMMERCE, *available at*, https://www.commerce.gov/about.
[3] *Id*.
[4] Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community*, (April 9, 2021), *available at* https://www.commerce.senate.gov/services/files/8EF2DE7F-E5AA-49ED-88B5-536F78840218.
[5] *Id*. at 8.
[6] *Id*. at 7.
[7] *Id*.
[8] *See, e.g.*, FY 2017 Congressional Submission, *available at* https://www.commerce.senate.gov/services/files/8EF2DE7F-E5AA-49ED-88B5-536F78840218.

Community, the unit lacked appropriate legal authorization to engage in any form of counterintelligence operation.

For nearly sixteen years, abuse of the Special Deputation program involved engagement in a variety of criminal and counterintelligence investigations, including ancillary activities like permitting agents to carry firearms, monitor electronic and wire communications, and conduct warrantless searches of office space and personal lockers on Department grounds. The unit even maintained a database to store information on foreign nationals and U.S. citizens.

In addition, the unit lacked internal policies defining the scope of its investigative authorities for most of its existence, which allowed it to become what whistleblowers described as a "gestapo." As a result, the unit investigated employees across the Department of Commerce and within the ITMS by designating them as threats to critical assets, often without reasonable suspicion that the subject posed a particularized threat or maintained connections to hostile foreign actors. This unchecked race-based targeting disproportionately impacted employees of Chinese ancestry.

The lack of meaningful oversight has allowed ITMS to conduct investigations without following best practices in line with proper law enforcement norms and expectations, including informing witnesses and subjects of their rights, or properly documenting investigative efforts, such as memorializing interviews or retaining notes in electronic case files. Few internal procedures existed to provide guidance on case management, which reportedly led to an abuse of the document classification process that shielded investigations from external review by other branches of government, including Congress.

The Department of Commerce largely funded the ITMS through a slush fund. Use of the "Working Capital Fund" sustained the unit's unlawful practices over time with minimal transparency. Poor resource management within the office resulted in a backlog of unresolved cases as well, depriving those under investigation of a fair process.

Similar concerns about ITMS's authority and investigative practices were reported to the Office of Inspector General at the Department of Commerce as early as 2017. Despite what appears to be clear evidence indicating abuse of the Special Deputation program, reprisal against current and former employees, and longstanding abuse of federal resources, no significant findings have been made by the Inspector General.

V. COMMITTEE INVESTIGATION

A. Investigations and Threat Management Service

The Investigations and Threat Management Service (ITMS) collaborates with the Office of Security at the Department of Commerce to enhance protection of the Secretary and the Herbert C. Hoover Building, among other facilities, primarily by identifying and assessing critical threats to the Department's mission, operations, and activities. The unit, based in Washington, DC, employs a small team of criminal investigators and maintains a satellite office in Boulder, Colorado. According to the Department of Commerce, the ITMS uses "the full range of investigative techniques permitted by law or regulation to identify [and] assess unreported or unrecognized threats to the Department's mission, operations or activities, including examining any initiative, project, program, process, function, or incident involving the Department [and] commence or coordinate investigations and operations to protect Departmental personnel, assets, and activities from recognized mission-critical threats."[9]

The unit operated under the Office of Security as the Investigations and Intelligence Program, Investigations and Intelligence Division, and the Investigations and Threat Management Division from 2005 to 2019. It became the Investigations and Threat Management Service in 2019. Although the purpose of separation from the Office of Security is unclear, whistleblowers reported that George Lee, Director of ITMS, proposed a change in organizational structure to enable the unit to conduct criminal and counterintelligence investigations with increased autonomy and reduced oversight from Department officials.

B. Abuse of Authority

The ITMS lacks the proper legal authority to conduct criminal investigations or engage in counterintelligence activities. Over the past sixteen years, the ITMS has operated as an investigative police force by relying on delegations of law enforcement authority from other federal agencies. None of those delegations supply the requisite authorization for ITMS to conduct criminal or counterintelligence investigations.

No statute provides the ITMS with law enforcement authority for investigating criminal matters or participating in counterintelligence activities. Early in its existence, ITMS officials even acknowledged that the unit had "no specific criminal investigative or public law enforcement authority."[10] Over the course of time, however, the ITMS interpreted a string of provisions and departmental orders defining the powers of the Department of Commerce in order to justify involvement in matters outside of providing protection to the Secretary and the Herbert C. Hoover Building. Those orders focused broadly on a delegation from the Secretary to the Office of Security, which enables agents to protect the "Department's assets, operations and personnel" as well as "assess any threat to the Department's mission or activities, and provide functional services

[9] Investigations and Threat Mgmt. Div., *Basic Agent Training Presentation*, https://www.commerce.senate.gov/services/files/7F85FBCD-446C-4798-AC5A-9237DFC79F47.
[10] Memorandum from George Lee, Office of Sec., Dep't of Commerce, to Rich Yamamoto, Dir. of Sec., Dep't of Commerce, (Apr. 13, 2005), https://www.commerce.senate.gov/services/files/7F85FBCD-446C-4798-AC5A-9237DFC79F47.

as required."[11] Without independent police powers to carry out this mission, the ITMS relied on delegated authorities from the U.S. Marshals Service to exercise law enforcement authority.[12]

I. Law Enforcement Delegations

Two primary types of law enforcement authorities are delegated to federal agents in the Department of Commerce. First, the Department of Homeland Security (DHS) is authorized to delegate authority to federal agents. DHS "stipulates the requirements for a designated Federal Department or Agency to be authorized to act on behalf of DHS in providing law enforcement or protective security officer services for the purpose of protecting Federal property and persons on the property." The delegation request form, accordingly, offers two types of authority:

- A ***law enforcement delegation*** is the delegation of law enforcement authority and power to another federal agency. This type of delegation is only for law enforcement authority and does not provide any authority for the requestor to procure protective security officers; or

- A ***protective security delegation*** pertains to the delegation of authority for another federal agency to use contract protective security officers for purposes of protecting Federal property and persons on the property. A protective security delegation allows the requestor to obtain protective security officers if the use of such protective security officers is consistent with FPS protective security requirements.[13]

An agent is only authorized to exercise powers under the type of delegation granted by the Department of Homeland Security, meaning the special delegation is a license for a specific purpose. The primary purpose of this delegation for agents in the Department of Commerce is for providing physical protection to the Herbert C. Hoover Building. According to documents reviewed by the Committee, for example, the type of authority delegated to agents operating within the ITMS was only for "protective security services." This allowed ITMS to "conduct[] investigations, on and off the property in question, of offenses that may have been committed against property owned or occupied by the Federal Government or persons on the property."[14] The delegation also allows agents to carry firearms and make arrests if necessary to fulfill the specified mission.[15] No known application sought a law enforcement delegation, which means the ITMS has been authorized only to provide physical protection to the grounds on which the Department operates under this delegation.

---

[11] *See also* 15 USC § 1512 ("It shall be the province and duty of said Department to foster, promote, and develop the foreign and domestic commerce, the mining, manufacturing, and fishery industries of the United States; and to this end it shall be vested with jurisdiction and control of the departments, bureaus, offices, and branches of the public service hereinafter specified, and with such other powers and duties as may be prescribed by law); 5 USC § 301 ("The head of an Executive department or military department may prescribe regulations for the government of his department, the conduct of its employees, the distribution and performance of its business, and the custody, use, and preservation of its records, papers, and property.)

[12] DEP'T OF COMMERCE, DOO 20-6, *available at*, https://www.osec.doc.gov/opog/dmp/archive/doo20_6archive.pdf.

[13] Dep't of Homeland Sec., *FPS Delegation of Authority: Request for Information* (May 2017), https://www.commerce.senate.gov/services/files/7F85FBCD-446C-4798-AC5A-9237DFC79F47.

[14] *See* 40 U.S.C § 1315(e).

[15] *See* 40 U.S.C § 1315(b)-(c).

Second, federal agents participate in the Special Deputation program offered by the U.S. Marshals Service, which provides a delegation of law enforcement authority for providing protection of government personnel and property.[16] Before exercising law enforcement powers associated with this delegation, agents must acknowledge that their "special deputation can only be exercised in furtherance of the mission for which he or she has been specially deputized."[17]

The Marshals Service originally offered this delegation for providing protective services to the Secretary of Commerce at the Herbert Hoover Building. Documents confirmed that the ITMS believed in the early 2000s that the Special Deputation "grant[ed] police powers only while protecting the Secretary."[18] Before the decade ended, however, the Marshals Service expanded the scope of its Special Deputation, permitting agents to use law enforcement powers for protecting the Department's "critical assets" as well.[19] The Marshals Service has not formally defined the meaning of critical assets, but ITMS officials originally understood that it covered only tangible assets like federal property and facilities.[20] ITMS leaders nonetheless directed agents to engage in a troubling variety of criminal and counterintelligence investigations to protect intangible assets, such as those related to economic intelligence, wire communications, online publications, employee relationships, and security clearances. Use of law enforcement powers to investigate these activities violated the authorized purpose of the Special Deputation program. Materials obtained by the Committee's Minority Staff clearly illustrates that the ITMS, using the authority of the Special Deputation program, authorized its agents to investigate offenses of the federal criminal code.

II. Abuse of the Special Deputation Program

The ITMS repeatedly abused the Special Deputation program by conducting criminal investigations into purported threats to the Secretary or the Department of Commerce. The Special Deputation, however, only allows agents to provide protection for the Department's "critical assets," meaning physical objects.[21] Although the ITMS is intended to serve a broader mission than the Secretary's protective detail, the range of law enforcement powers that ITMS agents exercised over an extended period of time investigating potential criminal violations fell far outside the scope of the Special Deputation.

As early as 2005, ITMS officials began directing agents to pursue criminal matters related to threats against the Secretary and *tangible assets* such as federal facilities and property.[22] They

[16] *See* 28 U.S.C. §§ 561, 566.
[17] *Id*.
[18] *Supra* note 10, at 2.
[19] *Id*. at 3. Lee ceded that delegations from the Department of Homeland Security, on the other hand, would be "at most available for the protection of property [and] persons on such property."
[20] Admissions by George Lee suggest the ITMS did not have the proper authority to engage in activities beyond providing protection to the Secretary and federal property. *See supra* note 10.
[21] U.S. Marshals Service, *Special Deputation Oath of Office, Authorization, and Appointment*, https://www.commerce.senate.gov/services/files/7F85FBCD-446C-4798-AC5A-9237DFC79F47. There is general agreement about the term's meaning across federal agencies. *See, e.g.*, 14 CFR § 401.7 (referring to physical property and facilities); 6 CFR §27.230 (describing critical assets as facilities and restricted physical areas).
[22] These investigations were likely covered by the USMS Special Deputation. The DHS deputation alternatively provided this authority.

claimed to agents that the unit had authority to probe "activities or items which if compromised would cause significant damage to U.S. economic advancement, the U.S. Government's ability to function, or Departmental functions in support of these concerns."[23] This vague mission is unusually broad for a unit without investigative police powers, especially since other federal agencies fulfill these objectives. Nonetheless, ITMS agents improperly exercised law enforcement authority by carrying firearms aboard commercial aircraft, conducting warrantless searches and seizures, performing custodial interrogations, and making arrests.

Without effective oversight from the Department or the Inspector General, the ITMS expanded its portfolio to include investigations about threats against *intangible assets* as well. In a letter to the Marshals Service, a senior ITMS official acknowledged that its expanding "responsibility requires the capability to provide security for such assets which may be inadequately protected or temporarily lack any protection, particularly for intangible assets that are not contained in a Department facility or assets demanding protection from a previously unrecognized, imminent, or evolving security threat."[24] In addition, the Special Agent Directive used by the Office of Security acknowledged that the ITMS regularly interprets "critical assets" to cover more than the protection of physical structures.[25]

Neither the Department of Commerce nor the ITMS defined what constitutes a "critical asset." Former ITMS agents claimed that the unit has maintained a classified inventory of tangible and intangible items that fall within the term's meaning, which has allowed officials to stretch the term to cover "any area where ITMS could assert law enforcement authority."[26] ITMS officials used this practice to justify involvement in a variety of criminal investigations unrelated to providing protective services simply by classifying the subject as a threat to a "critical asset."

Despite delegating law enforcement authority, the Marshals Service has not defined the term's meaning. Minority Staff engaged the Marshals Service to clarify the scope of Special Deputations for ITMS. After two months of refusing to answer this question, the Marshals Service requested a formal letter before issuing a response. As a result, Ranking Member Roger Wicker, along with Ranking Member Charles Grassley of the Judiciary Committee, sent the Marshals Service a formal letter on May 26, 2021, seeking to probe the Special Deputation program.[27] Although the request for information allowed officials sufficient time to comply, the Marshals Service failed to respond. The Marshals Service did provide a statement, however, to the *Washington Post*, describing the purpose of the Special Deputation as one solely "for protection of the Secretary of Commerce."[28]

---

[23] Memorandum from Lisa Casias, Dep. Assistant Sec. for Admin, Dep't of Commerce, to Office of the Inspector Gen., Dep't of Commerce (Dec. 20, 2018), https://www.commerce.senate.gov/services/files/640BDA8F-A7F0-483C-B541-C1F75DABDE5D.
[24] *Id*.
[25] *Id*.
[26] Interview with Clifton Dyer (Feb. 8, 2021).
[27] Letter from Sen. Roger Wicker, Ranking Member, S. Comm. on Commerce, Sci., and Transp., and Sen. Charles Grassley, Ranking Member, S. Comm. on the Judiciary, to Donald W. Washington, Dir., U.S. Marshals Serv. (May 26, 2021), https://www.commerce.senate.gov/services/files/2F09349F-6461-4185-A7C6-EC77ABE1BB2D.
[28] Shawn Boburg, *Commerce Department Security Unit Evolved into Counterintelligence-like Operation*, WASH. POST (May 24, 2021), https://www.washingtonpost.com/investigations/2021/05/24/commerce-department-monitoring-itms/.

It is unclear why the Marshals Service readily answered a media inquiry but refused to answer similar questions from Ranking Member Roger Wicker.

Criminal Investigations

Without a defined meaning of what constituted a critical asset from the Marshals Service, the ITMS conducted investigations typically reserved for domestic law enforcement agencies. Many were conducted in an overzealous manner whereby agents abused steps in the investigative process. In one instance, the ITMS investigated Sherry Chen, an award-winning, Chinese-born hydrologist employed at the Department, on charges of espionage and providing false statements after she allegedly downloaded and distributed unclassified information to a foreign national. Agents reportedly interrogated her for seven hours and told her she could never discuss the interrogation with anyone, including her superiors. In a lawsuit filed against federal officials, Chen said that ITMS agents "ignored exculpatory evidence throughout the interview, reached false conclusions without even a cursory investigation of underlying facts, and reported false results reflecting their racial and ethnic bias."[29] In this sense, Chen claimed that agents even provided her with paper to draft a statement and instructed her to write words they prepared after telling her that she did not need to consult with counsel. Chen said she felt compelled to draft the incriminating statement as instructed because investigators intimidated her and "left [her] with no choice."[30]

Several months later, ITMS agents prepared an investigative report and referred the matter to the Federal Bureau of Investigation's (FBI) counterintelligence division, as well as an "intelligence unit within the military."[31] The FBI collaborated with federal prosecutors who filed a criminal complaint against Chen in 2014. She was arrested, but Justice Department officials ultimately dropped all criminal charges weeks later.[32] In a subsequent proceeding before the Merit Systems Protection Board (MSPB), a federal administrative judge concluded that the information Chen shared with a Chinese national was "public information," noting that investigators "found no evidence that Ms. Chen had ever provided secret, classified, or proprietary information to a Chinese official or anyone outside of the agency."[33] Ms. Chen remains employed by the Commerce Department but remains on administrative leave while the government appeals her reinstatement by the MSPB.

In the final days of the Obama administration, the ITMS investigated Chunzai Wang, one of the world's foremost experts on oceanic climate change, based on his connection to organizations associated with the Chinese government.[34] Wang served as a research oceanographer in the National Oceanic and Atmospheric Administration (NOAA) in Miami, Florida at the time. Agents from the ITMS executed a search warrant at his home and interrogated him for hours, which

---

[29] Pl.'s Mot. to Am. Compl., Chen v. United States, No. 1:19-CV-00045 (S.D. Ohio, 2019), https://www.apajustice.org/uploads/1/1/5/7/115708039/chem_mot_to_amend_-_final.pdf.
[30] Video Interview with Sherry Chen (June 16, 2021).
[31] *Id*.
[32] Nicole Perlroth, *Accused of Spying, Until She Wasn't*, THE NY TIMES (May 9, 2015), https://www.nytimes.com/2015/05/10/business/accused-of-spying-for-china-until-she-wasnt.html.
[33] Pl.'s Am. Compl, Chen v. United States, No. 1:19-CV-00045 (S.D. Ohio, 2019), *available at* https://www.apajustice.org/uploads/1/1/5/7/115708039/chen_pfac_final_-_pdf.pdf.
[34] *See* John Pomfret, *Opinion: America's New — and Senseless — Red Scare*, WASH. POST (Mar. 8, 2018), https://www.washingtonpost.com/news/global-opinions/wp/2018/03/08/americas-new-and-senseless-red-scare/.

ultimately led federal prosecutors to charge him with accepting a salary from the Chinese government.[35] Following his conviction, the Justice Department announced that "while employed at NOAA, Wang entered into contractual agreements to work on China's Changjiang Scholars Program, Thousand Talents Program, and was also involved in China's 973 Program which mobilizes scientific talents to strengthen basic research in line with national strategic targets of the People's Republic of China."[36] For unclear reasons, prosecutors ultimately dropped five other counts and only sought a minimal penalty for remaining count. Wang's counsel noted:

> Your Honor, this is a — an unusual request as a prosecutor. I don't recall ever having a situation where — where the Government, you know, made this recommendation or we were in this posture. So it is unusual.[37]

At his sentencing hearing, U.S. District Court Judge Cecilia Altonaga acknowledged that Wang "made certain mistakes," but found it "regrettable" that prosecutors pursued the felony charge in in light of the evidence presented to the court.[38] Although Wang faced up to five years in prison, he served only one night after the prosecution's recommendation of no additional sentence.

Additional evidence confirms that the ITMS regularly sought to enforce federal criminal statutes. In one document, ITMS officials described to agents a broad range of offenses for which referrals to federal prosecutors could be made. Substantive offenses included racketeering, money laundering, and theft of government property, espionage, economic espionage, and computer fraud. More commonly, however, ITMS agents sought to charge targets of its criminal investigations with offenses such as obstruction, conspiracy, making false statements to federal agents, and resistance to search.[39]

Documents also suggest that ITMS officials contemplated criminal investigations into federal lawmakers, noting in a Special Agent Directive that "Members of Congress may not be arrested while Congress is in session and while attending, going to and from, sessions of Congress."[40] The ITMS has allegedly investigated at least one lawmaker, a former member of the U.S. House of Representatives, for submitting a letter to Secretary Wilbur Ross in late 2019 announcing opposition to procedures used by the Department in conducting the U.S. Census. The Committee reviewed no evidence that suggested the letter presented any semblance of a threat to the Secretary's safety or any federal physical structure.

---

[35] Press Release, Dep't of Justice, Former Research Oceanographer Sentenced for Accepting a Salary from the People's Republic of China (Feb. 22, 2018). https://www.justice.gov/usao-sdfl/pr/former-research-oceanographer-sentenced-accepting-salary-people-s-republic-china.

[36] *Id*.

[37] Hr'g Tr. 8, United States v. Wang, Case No. 17-cr-20449-CMA (S.D. Fla. 2018), *available at* https://www.committee100.org/wp-content/uploads/2018/03/USA-v-CHUNZAI-WANG-02-20-18-Original-Transcript.pdf.

[38] *Id*. at 20.

[39] *Supra* note 9.

[40] Dep't of Commerce, Office of Sec., *Special Agent Directive* (Aug. 1, 2013), https://www.commerce.senate.gov/services/files/7F85FBCD-446C-4798-AC5A-9237DFC79F47.

Investigating threats to the Secretary and the Commerce Department's assets—both tangible and intangible—ultimately led to the mutation of the ITMS into a rogue, unaccountable police force without a clear mission. Based on the evidence reviewed by the Committee, ITMS leadership either lacked the requisite training to determine what constituted a threat within the bounds of their authority to investigate, or willfully leveraged their own definition of "critical assets" to act as a counterfeit law enforcement body.

Oversight by the U.S. Marshals Service

According to several former senior officials with the Marshals Service, the Special Deputation program has experienced significant oversight and accountability challenges for decades. These challenges are not limited to the participation of the Department of Commerce. Evidence obtained by Minority Staff revealed structural deficiencies in the program that threaten the credibility of the Marshals Service in delegating law enforcement authority for acceptable and clearly articulated purposes.

One former program manager described a reorganization of the Special Deputation program in 2010, which revealed that the agency lacked awareness about the total number of active participants in the Special Deputation program.[41] Officials did not know how many individuals maintained active credentials and badges, or if the awarded badges and credentials were recovered following the expiration of the Special Deputation. The manager also described a review where officials determined that some individuals were granted a Special Deputation of law enforcement authority based solely on personal friendships with senior officials at the Marshals Service. Evidence of this activity included a "bag of badges" identical to sworn deputy U.S. Marshal badges in a closet on the Director's floor at the Marshals Service headquarters. Staff reported that the badges were for the Director's "special deputies," and senior officials gave other out badges out as "mementos."

III. Participation in Counterintelligence Activities

As the ITMS began regularly conducting criminal investigations without proper oversight from Department officials or the Inspector General, officials in the early 2010s began gathering intelligence on foreign nationals and U.S. citizens, as well as using counterintelligence tools. Despite lacking any form of legal authorization to conduct these operations, the Commerce Department even described the ITMS in a submission to Congress as an office that fulfilled objectives related to "counterintelligence, transnational crime, and counterterrorism" by investigating "serious threats to national security."[42] It is unclear to what extent the ITMS engaged in traditional counterintelligence activities like those conducted by agencies in the Intelligence Community.[43] The Department has publicly characterized a mission of this type for the unit, however, since the Obama administration.[44]

---

[41] Interview with Anonymous Former Official, U.S. Marshals Service (July 13, 2021).
[42] FY 2018 Congressional Submission, *available at* https://www.commerce.senate.gov/services/files/8EF2DE7F-E5AA-49ED-88B5-536F78840218.
[43] *See* Michael E. DeVine, Cong. Research Serv., R45175, Covert Action and Clandestine Activities of the Intelligence Community: Selected Definitions in Brief (June 14, 2019), https://fas.org/sgp/crs/intel/R45175.pdf.
[44] FY 2011 Congressional Submission, available at https://www.osec.doc.gov/bmi/budget/11CJ/DM_Congressional%20Submission,%202011.pdf.

Federal law provides clarity on which departments are authorized to gather intelligence and perform counterintelligence functions, especially when U.S. citizens are targeted. The National Security Act of 1947 broadly structured the federal government's intelligence-gathering capabilities, and a variety of subsequent executive orders detailed the goals, duties, and responsibilities with respect to collecting and sharing sensitive information.[45] According to Executive Order 12333, which President Ronald Reagan signed on December 4, 1981, counterintelligence is defined 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."[46] The Department of Commerce, however, is not listed as part of the Intelligence Community tasked with exercising counterintelligence tools or otherwise "conduct[ing] intelligence activities necessary for the conduct of foreign relations and the protection of the national security of the United States."[47]

Despite exclusion of the Department of Commerce from the Intelligence Community, ITMS officials told the Inspector General in late 2018 that the unit "associates, cooperates, and consults" with intelligence agencies through the Office of Executive Support (OES).[48] For years, OES served as the official liaison to these agencies, but according to whistleblowers, ITMS officials eventually saw the office as an impediment. In the final months of the Obama administration, the OES "became non-operational" after ITMS opened a number of investigations into the office's senior personnel without any apparent legitimate basis. To fill the void, the ITMS then assumed the role from OES as the Department's "principal representative" with the Intelligence Community, which officials confirmed in correspondence with the Inspector General in a memo dated May 21, 2019.[49] In addition, the position of Deputy Assistant Secretary for Security had not been filled in the Obama administration, despite its listing in the "Code of Federal Regulations as the [Commerce Department] official responsible for implementing the regulations and executive orders that deal with the classification, declassification, and public availability of national security information."[50] Although the Trump administration briefly filled the role with the appointment of John Costello, the position again became vacant in early January 2021.[51] This meant that the Department failed to perform any meaningful oversight of the ITMS relationship with agencies in the Intelligence Community as far back as 2016 with the exception of Costello's tenure.

---

[45] OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, REFERENCE BOOK – 1947 NATIONAL SECURITY ACT (2020), https://www.dni.gov/index.php/ic-legal-reference-book/national-security-act-of-1947.

[46] Exec. Order No. 12,333, 3 C.F.R. 200 (1981), *reprinted in* 50 U.S.C. § 401 app. at 44-51 (1982).

[47] *Id*.; Michael DeVine, Cong. Research Serv., U.S. Intelligence Community (IC): Appointment Dates and Appointment Legal Provisions for Selected IC Leadership, (Mar.19, 2019), https://fas.org/sgp/crs/intel/IF10538.pdf

[48] *Supra* note 23. In a document submitted to Congress before this investigation began, the Biden administration referred to the ITMS as the "primary liaison with the wider Intelligence Community." Dep't of Commerce, *FY 2021 Working Capital Fund Advances and Reimbursements Final Handbook*, *available at* https://www.commerce.gov/sites/default/files/2021-03/DM_FY_2021_Final_WCF_and_AR_Handbook.pdf

[49] Memorandum from Richard L. Townsend, Dir. of Sec., Dep't of Commerce, to Office of the Inspector Gen., Dep't of Commerce (May 21, 2019), https://www.commerce.senate.gov/services/files/640BDA8F-A7F0-483C-B541-C1F75DABDE5D.

[50] *Id*. *See generally* 15 CFR § 4.10.

[51] According to senior officials at the Department of Commerce, the Biden administration filled the position in July 2021.

Correspondence with the Inspector General also revealed that the National Counterintelligence and Security Center (NCSC), a component of the Office of the Director of National Intelligence (ODNI), completed multiple reviews of ITMS counterintelligence activities during the Obama administration.[52] The NCSC acknowledged that reviewing a unit outside the Intelligence Community was unusual, but noted the importance of ITMS involvement in counterintelligence operations since "several critical assets" in the Commerce Department "may be of interest to foreign intelligence services."[53] Failing to recognize the limited legal authority of ITMS involvement in counterintelligence matters, the NCSC reported that the unit's activities represented "excellent initiatives" with "potential applications elsewhere in the counterintelligence community."[54]

After evaluating this evidence, Ranking Member Wicker, with Ranking Member Charles Grassley of the Judiciary Committee, sent a formal request for information to Director of National Intelligence Avril Haynes on June 9, 2021.[55] The letter sought to probe the relationship between the ITMS and the Intelligence Community. ODNI refused to provide a response, precluding the Commerce, Science, and Transportation Committee from performing effective oversight of any involvement in joint activities with the ITMS.

The ITMS operated as if it had independent authority to engage in counterintelligence operations. In particular, the ITMS maintained it was capable of "conducting protective intelligence investigations" based on authority delegated to the Office of Security from the Secretary of Commerce.[56] These investigations targeted "mission critical threats," which are defined by the Commerce Department's Security Manual of Security Policies as "a person, entity, or circumstance that creates a security concern by having the actual or constructive intent and capability to interfere in an unlawful or dangerous manner with the Department's mission."[57] The threat spectrum ranged from organized criminal activity and foreign intelligence services to non-state actors, extremist groups, and unstable persons.[58] Even significant events, "such as geopolitical crises, natural disasters, and pandemics," could purportedly compromise the Department's mission and qualify as a mission critical threat justifying the use of counterintelligence tools.[59]

Relying on the Special Deputation from the Marshals Service for baseline authority, the ITMS believed the vagueness of "mission critical threats" provided enough latitude to investigate any

---

[52] *Id*. These reviews occurred in 2011, 2013, and 2016. Before NCSC came into existence in 2014, the reviews were conducted by the Office of the National Counterintelligence Executive, according to documents provided to the Inspector General by ITMS officials.
[53] *Id*. The NCSC purportedly told the ITMS that it was the "first time [they] reviewed the counterintelligence program of a department or agency not in the Intelligence Community."
[54] *Id*.
[55] Letter from Sen. Charles Grassley, Ranking Member, S. Comm. on the Judiciary., and Sen. Roger Wicker, Ranking Member, S. Comm. on Commerce, Sci., and Transp., to Avril Haynes, Dir., Office of the Dir. of Nat'l Intel. (June 9, 2021), https://www.commerce.senate.gov/services/files/2F09349F-6461-4185-A7C6-EC77ABE1BB2D.
[56] DEP'T OF COMMERCE, DOO 20-6, *available at*, https://www.osec.doc.gov/opog/dmp/archive/doo20_6archive.pdf.
[57] DEP'T OF COMMERCE, MANUAL OF SECURITY POLICIES AND PROCEDURES 323 (Feb. 07, 2017), https://www.governmentattic.org/24docs/DOCmanSecPolProced_2012-2016.pdf.
[58] *Id.*
[59] *Id.*

matter purportedly related to national security. Former ITMS Agent Martin Kehoe claimed in a written memo that the ITMS used the broad definition "to initiate investigations . . . into almost every departmental activity" because "[t]he definition is so broad anyone could construe almost anything with a Departmental nexus as a mission critical threat."[60] He went on to claim that

> [t]he [legal] authorities, which are not statutory, have led to ITMD conducting counterintelligence, protective intelligence (PI), transnational organized crime, counter-terror, insider threat investigations, and general threat management activities. SAC Lee has made it clear on numerous occasions that he would not seek statutory authority for his unit because many of the functions are already provided by existing law enforcement agencies who may not allow ITM[S] to retain those authorities. The [Special] Deputation was designed as a way around statutory authority that is so general in nature, ITMD can operate like the FBI, CIA, [and] NSA with very little oversight.[61]

In essence, the broad meaning of mission critical threats allowed the ITMS to treat its authority as "a fluid concept."[62] Without safeguards in place to monitor the unit's exercise of law enforcement powers, the ITMS began conducting operations as an appendage to the Intelligence Community.

The ITMS used a troubling variety of tactics to gather intelligence. According to whistleblowers, ITMS agents regularly searched the office space of employees suspected of wrongdoing, which required forced entry through lock picking.[63] These covert searches involved identity-concealing tactics, including the use of facemasks, latex gloves, and shoe coverings.[64] The unit also seized work phones and computers to perform digital content searches, practices that continued until the Department required the unit to cease investigative activities in March 2021. Former ITMS agents claim that these activities often happened without any articulable evidence to indicate that the employee maintained suspicious connections with foreign actors or otherwise posed a threat to the Department.

In addition to searches of physical premises, whistleblowers claim that the ITMS regularly searched Department servers and monitored employee email accounts to scan for evidence of foreign influence as early as 2014. In particular, these searches began focusing on uncovering connections between Department employees and actors within the Chinese government. To achieve this end, whistleblowers allege that the ITMS specifically targeted multiple divisions with a comparably high proportion of Asian-American employees.

Whistleblowers claim, for example, that agents were directed to run ethnic surnames through secure databases even in the absence of evidence suggesting potential risk to national security, indicating that immutable characteristics served as a pre-text for initiating investigations. Documents show that the ITMS also ran broad keyword searches of email accounts using a broad

---

[60] Memorandum from Martin Kehoe, to John Costello, Dep. Assistant Sec'y. of Intel. and Sec., Dep't of Commerce (Sept. 24, 2020), https://www.commerce.senate.gov/services/files/7F85FBCD-446C-4798-AC5A-9237DFC79F47.
[61] *Id*. at 2.
[62] *Id.* at 1.
[63] Interview with William Bent (Feb. 9, 2021).
[64] *Supra* note 28.

variety of terms and phrases in Mandarin Chinese, such as "state key laboratory," "overseas expert consultant," "Ministry of Science and Technology," "funding support," "government support," and "highly secret."[65] Multiple whistleblowers claimed that the unit worked with officials at the CIA and FBI to devise the list of search terms and review the results.

These searches also targeted references to individuals in a variety of science-based talent recruitment schemes sponsored by the Chinese government, namely the Thousand Talents and Hundred Talents programs. One whistleblower even reported that "if a Chinese university emails a DOC researcher to submit an application"[66] for these programs, then ITMS opened a case into the Department employee.

One former senior Commerce Department official described the indiscriminate targeting of Chinese-Americans as a "fine line between extra scrutiny and xenophobia, and one that ITMS regularly crossed."[67] This official also discovered a case into a Chinese-American employee at the Department left open for four years without any indication of investigative diligence to close the matter, claiming that the ITMS "targeted her purely because of her ethnic Chinese origin."[68] The official also believes that ITMS leaders directed agents to "launch the investigation for the purpose of raising the heat so high that she became radioactive and would have to leave the Department," despite no indication that she presented a national security threat after her emails had been pulled and agents surveilled her on Department premises and at her home.[69] Citing tense relations between the U.S. and Chinese governments, the official believes that the ITMS sought aggressively to counter any attempt at espionage from within the Department.

Former ITMS agent Chris Cheung similarly claimed in a memo to former Secretary Wilbur Ross dated January 2021 that officials "discriminately targeted ethnic Chinese foreign guests [and] visitors and employees as well as other ethnic personnel."[70] He wrote that "[w]hen investigations on these ethnic personnel are inconclusive, [ITMS leadership] refuse[d] to allow agents to close the cases."[71] Other whistleblowers confirmed this claim, suggesting that an audit of managerial systems revealed that many dismissed cases into Asian-American employees, including individuals of Chinese and Middle-Eastern descent, were even categorized as "terrorism-related." This practice meant that multiple employees of color likely experienced protracted administrative processes to clear their names of suspected wrongdoing.

The ITMS targeted members of the general public—meaning U.S. citizens—as well. One whistleblower claims that the ITMS regularly performed "intelligence checks" on individuals associated with foreign visitors to Department of Commerce buildings. These searches involved querying both foreign nationals and U.S. persons in classified databases to determine whether they presented a threat to the Department, even without evidence indicating suspicious or malicious

[65] Investigations and Threat Management Service, *S-Searches* (Created Aug. 10, 2015). Publicly unavailable.
[66] Memorandum from Chris Cheung, Dep't of Commerce, to John Costello, Dep. Assistant Sec'y for Intel. and Sec. (Sept. 22, 2020), https://www.commerce.senate.gov/services/files/7F85FBCD-446C-4798-AC5A-9237DFC79F47.
[67] Phone Interview with Chris Cheung (Apr. 8, 2021).
[68] *Id.*
[69] *Id.*
[70] Email from Chris Cheung, Dep't of Commerce, to Wilbur Ross, Sec'y, Dep't of Commerce, (June 21, 2019), https://www.commerce.senate.gov/services/files/7F85FBCD-446C-4798-AC5A-9237DFC79F47.
[71] *Id.*

intentions. The whistleblower claimed that ITMS officials understood that these searches likely amounted to the "blatant disregard of constitutional rights" because agents never obtained any form of legal authorization to monitor or surveil citizens.[72] Minority Staff has not been able to ascertain how ITMS gained access to classified intelligence databases as reported. According to senior law enforcement and intelligence officials, access requires both the proper authority and a sufficient justification.

In early 2020, the ITMS began surveilling social media activity to monitor accounts that posted commentary critical of processes used to conduct the U.S. Census as well.[73] ITMS leadership reportedly sought to display the division's investigative capabilities to actors in the Intelligence Community by linking those accountholders to disinformation campaigns orchestrated by foreign governments. This meant that any account criticizing the Census opened the door for ITMS to consider the commentary threatening to a "critical asset," which allowed the unit to open a case and exercise investigative tools against the accountholder. To this end, dozens of posts were logged in a spreadsheet called the Social Media Tracker.[74] The spreadsheet shows that investigators completed "high-side" checks—meaning searches on secure classified databases—on the majority of posts it tracked, despite having unclear authority from the Intelligence Community to use these databases for this purpose.[75]

Many monitored accounts published commentary on Facebook and Twitter. In particular, ITMS officials tracked posts made by the U.S. Census Bureau's official Facebook page encouraging participation in the 2020 Census. The critical comments from members of the public cited the role of COVID-19 and the impact of undocumented persons as factors that made the Census illegitimate. One user, for example, commented the following: "The census takers they hire especially in rural areas like mine, are often older highly racist white people on fixed incomes trying to make some extra scratch. They fill the census out however they like, do not show you the answers, and if you refuse to let them in your home, they threaten to put you in jail and your kids in foster care."[76] ITMS officials also flagged a variety of posts on Twitter that purportedly spread disinformation about the Census. One account posted, "I.C.E. is coming for the illegals. They'll track you. Please fill out the census."[77] Another said, "The census counts illegals to give Democrats more representation in Congress. Boycott the census."[78] The majority of monitored Twitter accounts had fewer than one-hundred followers.

ITMS officials then reportedly forwarded the spreadsheet to the Foreign Influence Task Force of the FBI and the Office of Intelligence and Analysis at the Department of Homeland Security to elevate the purported threat posed by accountholders who questioned the integrity of the Census.[79]

---

[72] Video Interview with Bruce Ridlen (Apr. 1, 2021). Improper use of intelligence resources against U.S. citizens may be a criminal violation under 50 U.S. Code § 1809.
[73] *Id*.
[74] Investigations and Threat Management Service, *Social Media Tracker* (July 7, 2021). Publicly unavailable.
[75] *Id*.
[76] *Id*.
[77] *Id*.
[78] *Id*.
[79] Memorandum from George Lee, Investigations and Threat Mgmt. Serv., Dep't of Commerce, to Office of Intel. and Analysis, Dep't of Homeland Sec.; Memorandum from George Lee, Investigations and Threat Mgmt. Serv.,

No further action was taken after officials concluded that the comments consisted of protected free speech and presented no threats to national security or the Department's mission. Even though the posts in the Social Media Tracker contained no threatening content, none of the ITMS investigations into these accountholders had been closed as of late 2020.

IV. Legal Authorities Memorandum

For more than a decade, the ITMS directed agents to engage in law enforcement activities with knowledge that no legal basis existed to support them. In a memo from 2005, George Lee acknowledged that the ITMS "may lack legal authority to conduct an appreciable portion of its investigative efforts, particularly criminal investigations."[80] Based on this assessment, the memo offered multiple actions that ITMS should take in order to "legitimize" its exercise of law enforcement authority.[81] This included obtaining broader deputations from the Department of Justice, executing an agreement with the Office of Inspector General regarding the use of expanded investigative powers, and revising the institutional charter of ITMS to include criminal investigations as an explicitly authorized function. Lee even warned that if the Department failed to take these actions, the ITMS could one day face "sanctions from the Department of Justice and Homeland Security, OIG investigation, or revocation of current special deputations for Secretarial Protection and building security."[82] He even predicted that agents could face "serious criminal and civil liability," including charges of "impersonation, theft, assault, and false imprisonment," as well as "vulnerability to a *Bivens* action."[83]

No new authorities exist nearly sixteen years later than at the time Lee authored this memo. In 2017, Lee requested that the Commerce Department's Office of General Counsel produce an opinion discussing the legal authorities that authorize the ITMS to engage in law enforcement activities. Acting Deputy General Counsel Michelle D. McClellan drafted an informal email opinion. McClellan acknowledged the lack of explicit authority for ITMS to conduct law enforcement operations, but acknowledged the delegated authority from the unit's participation in the Special Deputation program.[84] The opinion concluded, however, that the deputation provided law enforcement authority solely "for purposes of protecting the Secretary and the Department."[85] Despite this understanding, Commerce Department officials allowed Lee and the ITMS to continue operating without proper authority.

Key Findings

The ITMS has always lacked the proper authority to conduct criminal or counterintelligence investigations, which led to chronic abuse of the Special Deputation program. For the entirety of

---

Dep't of Commerce, to Fed. Bureau Investigation, Foreign Influence Task Force, *available at* https://www.commerce.senate.gov/services/files/2CA1AF46-ABDC-4A14-B587-E1518F81BCE3

[80] *Supra* note 10.

[81] *Id.*

[82] *Id.*

[83] *Id.*

[84] Email from Michelle McClellan, Office of Gen. Counsel, Dep't of Commerce, to George Lee, Dir., Investigations and Threat Mgmt. Serv. (Nov. 28, 2017), https://www.commerce.senate.gov/services/files/7F85FBCD-446C-4798-AC5A-9237DFC79F47.

[85] *Id.*

the unit's existence, agents engaged in law enforcement activities outside the scope of the delegated authority for providing protective security services.

C. MISMANAGEMENT

The Investigations and Threat Management Service (ITMS) has suffered from chronic mismanagement for more than a decade. Whistleblowers claim that a culture of carelessness has defined the unit, identifying multiple managerial deficiencies that paralyze the division's ability to manage its caseload in line with industry standards. Leaders of the ITMS reportedly maintained these structures to centralize power over the unit's caseload, which resulted in abuses ranging from poor due diligence to the overclassification of documents.

Case Management System

The ITMS reportedly does not maintain a central case management system that meets acceptable standards. Former ITMS agents claim that only a Microsoft Excel spreadsheet contains data on each opened case, which includes personally identifiable information and other protected information without proper safeguards in place to preserve confidentiality.

Due to the dysfunctional nature of the spreadsheet database, cases reportedly remain open for years without update, in part because of an inability to upload or review documentation. One whistleblower even alleges that the spreadsheet allows agents to record the opening of sensitive investigations where "case notes begin on serious, time-sensitive allegations," but additional updates are not listed because information sharing is unworkable using the system in place. The system lacks the security required for use in any credible law enforcement unit because any user can add, change, or delete information from the spreadsheet at will.

One former senior official even described the network as a "vanity project" designed to showcase an unusual volume of open cases rather than facilitate a user-friendly system for agents to use in processing them. The official said leadership of the ITMS is more interested in appearing productive to retain the ability to investigate a wide variety of purported threats with broad discretion—and continue receiving funding from Congress—than processing cases within an acceptable period of time.

Overclassification

The ITMS reportedly does not maintain a central classification guide to determine the proper clearance levels for documents generated or obtained by agents. Whistleblowers observed officials arbitrarily labeling categorizations on documents without any formal process in place, which allows the unit to categorize documents it wishes to block from public view as "classified." In many cases, classification labels were allegedly even handwritten instead of digitally imprinted or stamped. These practices contravene the expectations of federal government entities tasked with handling sensitive information.[86]

[86] *See, e.g.*, Jennifer Elsea, Cong. Research Serv., RS21900, *The Protection of Classified Information: The Legal Framework* (May 18, 2017), https://fas.org/sgp/crs/secrecy/RS21900.pdf; Dep't of Commerce, Office of Sec., *Classification Management*, *available at* https://www.commerce.gov/osy/programs/information-

Classified Network

The ITMS allegedly used a classified IT network (CNET) for improper purposes, among them self-preservation.[87] According to multiple whistleblowers, the CNET contains over 95% unclassified material, including the majority of information obtained by agents as investigations unfold. Whistleblowers claimed that officials structured it primarily to store information for the purpose of blocking access to outside entities. This practice purportedly protects the ITMS from Freedom of Information Act (FOIA) requests and lets the unit conduct operations without fear of mandatory disclosures required by evidentiary rules in criminal cases that proceed through the nation's judicial system.

In addition, the unit reportedly uses the Joint Worldwide Intelligence Communications System (JWICS), which houses top secret and sensitive but unclassified information. The system allows the Department of Defense and agencies in the Intelligence Community to transmit classified information using a secure domain. The Department of Commerce, however, is not officially part of the Intelligence Community. It is unclear what authority the ITMS exercised to gain access to this system.

Internal Procedures

Until mid-2020, the ITMS lacked clearly defined internal policies and procedures.[88] The unit allegedly operated for more than a decade without providing guidance to agents on administrative processes ranging from assignment management to handling records containing sensitive information.

In addition, the ITMS operated without clearly detailed procedures for exercising law enforcement powers, including guidelines for carrying a firearm, using force, and making arrests, for much of its existence. Until mid-2020, the unit even lacked clearly defined procedures for conducting interviews and interrogations, administering constitutional rights to interviewees, handling evidence, engaging in undercover operations, requesting documents from partner agencies, and protecting the Department against cyber-related threats. In the words of one whistleblower, the unit has been "allergic to every basic tenet of law enforcement."[89] The chart below shows the status of internal policies as of July 2020.[90]

---

security/classification-management. *See also* Office of the Inspector Gen., Dep't of Commerce, OIG-13-031-A, *Classified Information Policies and Practices at the Department of Commerce Need Improvement* (Sept. 30, 2013), https://fas.org/sgp/othergov/doc-roca.pdf.

[87] Memorandum from Clifton Dyer, Supervisory Special Agent, to John Costello, Dep. Assistant Sec. for Intel. and Sec., Dep't of Commerce (Aug.7, 2020), https://www.commerce.senate.gov/services/files/7F85FBCD-446C-4798-AC5A-9237DFC79F47.

[88] *Id*.

[89] Phone Interview with Jason Groves (Apr. 21, 2021).

[90] Investigations and Threat Management Service, *Standard Operating Procedures* (Sept. 2020), https://www.commerce.senate.gov/services/files/7F85FBCD-446C-4798-AC5A-9237DFC79F47.

POLICY	Draft Status
I. MISSION	Drafting
II. GENERAL STANDARDS AND USE OF AUTHORITIES	Complete
III. RESOURCES	
A. Organization	
i. Fitness and Wellness	Complete
ii. Training	Drafting
iii. Field Training	Drafting
iv. Law Enforcement Availability Pay	Complete
v. Telework	Complete
B. On/Off-boarding of Personnel	Researching
C. Personnel Development	Researching
D. Facilities	Researching
E. Vehicles	Drafting
F. Property	Drafting
IV. ADMINSTRATIVE MANAGEMENT	
A. Organization	Complete
B. Assignment Management	Complete
C. Case Management System	Researching
D. Information & Records	
i. Sensitive Information Handling	Complete
ii. Record Retention	Complete
V. PERFORMANCE MANAGEMENT	
A. Planning, Reviews and Metrics	Drafting
VI. LAW ENFORCEMENT ACTIVITIES	
A. OPSEC	Researching
B. Arrest Procedures	Drafting
C. Use of Force/Weapons	Revision in progress
D. First Aid	Researching
E. Pursuit	Complete
VII. INVESTIGATIVE ACTIVITIES	
A. Intake	Complete
B. Inquiry	Complete
C. Investigation	Complete
D. Evidence Collection	Complete
E. Investigative Techniques	
i. Evidence Handling and Storage	Complete
ii. Interviews and Interrogations	Complete
iii. Cooperative Sources	Researching
iv. Undercover Operations	Researching

v. Research and Analysis	Researching
vi. Document Requests & Covers	Researching
vii. Legal Processes	Researching
F. Case Presentation	Drafting
G. Cyber	Drafting
VIII. THREAT MANAGEMENT ACTIVITIES	
A. Recommendations	Drafting
IX. SPECIAL ACTIVITIES	
A. Analysis	Researching
B. Strategic Threat Briefing	Researching
C. COOP/COG	Researching

According to former Supervisory Agent Bruce Ridlen, the ITMS intentionally operated "ad hoc" for more than a decade. Ridlen claimed that unwritten policies and informal procedures allowed ITMS to "operate in the gray area," meaning involvement in matters without first obtaining the proper authorization.[91]

Many of these practices changed, however, after the Trump administration installed John Costello as the Deputy Assistant Secretary for Intelligence and Security. Costello reportedly directed subordinates to create a centralized policy manual to articulate the unit's mission and define the scope of law enforcement powers available to agents in order to prevent additional abuses of power. His departure from the Department in early January 2021, however, prevented many of these policies and procedures from taking effect.

Key Findings

Poor management has allowed the ITMS to operate outside the norms of the law enforcement community. Deficient policies and procedures outlining the unit's investigative capabilities led to repeated instances of malfeasance, including the purposeful prolonging of investigations, unauthorized use of secured messaging systems, and overclassification of documents to protect the unit from outside scrutiny.

D. Lack of Training and Experience

Agents in the Investigations and Threat Management Service (ITMS) underwent unaccredited training that failed to meet the needs of an investigative unit tasked with providing protective security. The Basic Agent Training (BAT) offered to the small group of agents not only demonstrated the ITMS Director's lack of law enforcement knowledge but also featured courses better fit for agents training to join the clandestine service.

Many agents—including those with military, law enforcement, and counterintelligence experience—claimed that the BAT course in the Shenandoah Valley of Virginia failed to meet

[91] Video Interview with Bruce Ridlen (Apr. 1, 2021).

basic standards of federal agent training. They noted, for example, that trainees normally operate in a controlled environment with simulated weapons and close instructor supervision. Agents described the course taught by ITMS Director George Lee, however, as threatening to public safety. Trainees were tasked with following Lee as the "rabbit" at high rates of speed on rural two-lane roads in an area lacking cellular coverage, an unsanctioned exercise completed in government-owned vehicles.[92] Certain training simulations even involved "role players," recruited by Lee to confront "armed [ITMS] participants without their knowledge," reportedly in banks and government facilities.[93] Former ITMS Agent Chris Cheung described the experience as "the most reckless and unsafe training I have ever attended."[94]

Lee also taught courses on forensic analytics, despite lacking any demonstrable subject-matter qualifications, including a seminar on handwriting analysis. One whistleblower with previous training in this area reported that it was clear Lee did not understand the topic. Following two weeks of training, which cost taxpayers tens of thousands of dollars, no trainee passed the course. These training sessions lacked any form of accreditation, meaning it is likely that Lee made them up.

Aside from these deficiencies in agent training, George Lee himself failed to meet the basic training requirements expected of a federal Criminal Investigator. The Department of Commerce employs George Lee as a Criminal Investigator under the Office of Personnel Management's Classification System, referred to colloquially as an "1811." Documents reviewed by Minority Staff suggest Lee has not completed the requisite training generally required for classification as an 1811. It also appears that Lee has not completed a Protective Service Operations Training Program, or an equivalent training, as required by the Marshals Service's Special Deputation program to exercise law enforcement authority.

Key Findings

The ITMS provided an unaccredited Basic Agent Training (BAT), which endangered the safety of participating agents and the general public. In addition, ITMS Director George Lee lacked the proper qualifications to lead a criminal investigative program.

E. EMPLOYEE TARGETING

The ITMS investigated employees at the Department of Commerce despite minimal, if any, evidence to suggest they presented a threat to the Secretary or "critical assets." The motivation behind many of these investigations remains unknown, although the unit reportedly sought to investigate highly visible employees to display its investigative capabilities. In other instances, ITMS officials purportedly opened investigations for purposes of intimidation or retribution, creating the allusion that an individual was under investigation when, in fact, no threat existed to Department personnel or property. These investigations largely targeted employees within the ITMS and often resulted in their separation from the Department.

[92] *Supra* note 60.
[93] *Id*.
[94] *Supra* note 66.

Internal Targets

ITMS officials launched retributive investigations into personnel who openly challenged the validity of the unit's investigative practices or questioned whether proper authorities existed to conduct them at all. Senior officials, including George Lee, Thomas Valentine, and Richard Townsend, allegedly sought to entrap subordinates viewed as disobedient and disloyal in administrative inquiries, often issuing probationary periods to employees who challenged the lawfulness of the unit's practices.

Officials retaliated against employees unwilling to engage in practices they viewed as inappropriate or unlawful. According to whistleblowers, agents began raising questions about the Special Deputation program, in particular, as early as the mid-2010s. They reported that officials either dismissed employees—including administrative and investigative personnel, as well as contractors—unwilling to engage in a variety of extralegal activities, or made conditions so difficult that employees had little choice but resign. ITMS officials searched computers, cell phones, and office space of employees who had separated from the unit, often "discovering classified material in unclassified areas."[95] Whistleblowers claimed, however, that officials retroactively altered the classification of documents left behind by former employees, allowing the Department to initiate post-employment disciplinary proceedings with penalties that included revocation of security clearances.

In one example, the ITMS began investigating John Costello, who had been installed to establish internal controls on the unit, after his departure as Deputy Assistant Secretary for Intelligence and Security in early 2021. Costello became the subject of an investigation into whether employees leaked "sensitive information" to him following his resignation from the Department. In an email chain, ITMS officials used the derogatory codename "Bone Chip" to reference Costello, a veteran whose physical ailment requires the use of a cane for mobility. In response to the allegation against Costello, the ITMS convinced Director of Security Richard Townsend to "suspend access" for three Department employees to sensitive compartmented information facilities (SCIFs) at the Herbert C. Hoover Building, despite no evidence suggesting a breach of security protocols or leaked classified information. Each of the employees was favorably associated with Costello during his tenure at the Department.

The ITMS then opened an investigation into one of the employees, a detailee from another federal agency, whose clearance it had restricted. The detailee is a decorated employee who has maintained a security clearance for several years. When the Department directed the detailee to submit to an interview with ITMS agents, the detailee declined because the unit refused to provide a reason. The employee's detail to the Department of Commerce has ended, but the extent of damage done by ITMS remains unknown. ITMS never explained its reasoning for restricting the detailee's clearance, but the detailee will have to explain the matter in future clearance reinvestigations.

Intimidation and fear of reprisal from within the ITMS allowed the unit to investigate matters beyond providing protective security. By targeting employees unwilling to operate outside the bounds of authority, George Lee built a senior team over time who largely refrained from

[95] Video Interview with Bruce Ridlen (Mar. 18, 2021).

questioning his motives or tactics. Those who crossed him were "blackmailed and blacklisted," prompting one former ITMS agent to draw comparison with J. Edgar Hoover—the longtime director of the FBI who amassed intelligence on purportedly subversive federal employees at the outset of the Cold War.[96]

Departmental Targets

Across the Commerce Department, the ITMS often targeted employees renowned in their professional fields, reportedly to display the unit's ability to uncover purported "threats" within the civil service. A troublingly high quantity of these investigations appear to have lacked any articulable suspicion that the target presented any credible threat. Overzealous and overbroad investigations, which focused on factors related to the subject's federal security clearance, often failed to reveal misconduct or threatening association with hostile foreign actors. In many cases, these investigations targeted subjects with Chinese or Southeast Asian ancestry.

ITMS officials improperly influenced the federal government's procedure for reviewing security clearances held by Commerce Department employees. President William J. Clinton signed an Executive Order in 1995 establishing a uniform protocol for administering a personnel security program, which determines access to classified information for federal employees.[97] The order provides a formal procedure for reviewing new clearances, as well as one for existing clearance-holders. Section 5.2 requires that the government provide an employee who undergoes a review of access determination with a "comprehensive and detailed" explanation in writing about the basis for the conclusion and documents relevant to the adjudication through the Freedom of Information Act (FOIA) within 30 days, as well as inform the employee of their right to counsel and allow the employee a reasonable opportunity to appeal the determination.[98] When the ITMS launched investigations into background factors relevant for an employee's clearance, the agents in charge––and the agencies who adjudicated the claims they flagged—took few, if any, of these steps.

One subject, a former Special Agent in the Bureau of Industry and Security (BIS), received a medal from Secretary Wilbur Ross shortly before the unit initiated a security clearance investigation based on unidentified evidence. The Special Agent believed the investigation focused on a personal relationship with a Ukrainian national after discovering that a source reported to government officials that the foreign individual worked for Russian intelligence. The Inspector General of the Navy declined to open a formal inquiry. The matter was reviewed as part of the subject's background re-investigation, however, which was favorably adjudicated. Nonetheless, the ITMS opened a subsequent investigation years later, despite the absence of new details necessitating an additional review. Officials never disclosed the purpose of the investigation. During an interrogation that lasted three hours, however, the ITMS questioned the Special Agent's relationship with Russian government officials and even accused the Special Agent of helping a former Russian spy seek employment in the United States. ITMS officials also suggested the Special Agent to undergo a polygraph exam and consent to a search of a personal email account after discovering that the Special Agent sent three emails containing unclassified content from a

[96] Video Interview with Martin Kehoe (Apr. 19, 2021).
[97] Exec. Order 12968, *Access to Classified Information*, 60 Fed. Reg. 40,245 (Aug. 7, 1995), *available at* https://www.dni.gov/files/NCSC/documents/Regulations/EO_12968.pdf.
[98] *Id.*

government device. The emails reportedly contained only administrative content related to a presentation the Special Agent intended to deliver in a professional capacity overseas.

The BIS hired the Special Agent through the Excepted Service before the ITMS investigation began, meaning the individual worked on probationary status at the time.[99] At the end of the probationary period, ITMS officials sought the Special Agent's termination for unspecified reasons. The Department, at the direction of the Office of General Counsel, revoked the Special Agent's security clearance. Officials subsequently pressured the agent into signing a separation agreement rather than accept termination. Officials extended the offer on a weekday evening and it expired early the following morning. This prevented the Special Agent from first obtaining legal counsel. The Special Agent provided a signature under duress and separated from the Department.

A separate case confirms that the ITMS improperly investigated claims previously adjudicated by departments across the federal government when issuing security clearances. The ITMS launched an investigation into a foreign-born military veteran whose clearance had been granted by the Department of State before the individual accepted a position at the Commerce Department.[100] ITMS launched this investigation after the individual self-reported harassment from conspiratorial groups online. As a result of this investigation, the individual's security clearance transfer experienced a two year delay. Department officials ultimately concluded the allegations raised by the ITMS lacked merit, and the individual's clearance transferred from the Department of State intact.

Early in the Obama administration, the ITMS investigated a decorated Department official reportedly suspected of affiliating with terrorists while serving overseas. The official had won a medal from the U.S. Armed Forces based on exemplary service as part of the Intelligence Community. At some point after joining the Department, the ITMS initiated an unprompted background investigation into the official's foreign contacts and professional experiences abroad, as well as details about the mosque attended by the official. This information had already been reported, investigated, and cleared as part of the individual's background investigation.

Agents never explained the basis of their investigation. Nonetheless, they alluded in the final interrogation that ITMS officials understood that no actual connection with terrorists existed. Despite this admission, the investigation prevented the official from transferring a previously obtained security clearance to the Department based on a purported "threat of foreign influence." This labeling not only blocked the official from career advancement within the Department but it impugned the reputation of an honorable public servant. Notably, the original agency later completed a favorable background reinvestigation, clearing the official of wrongful association with hostile foreign actors.

ITMS officials also investigated a dexterous attorney in the Office of General Counsel at the Commerce Department. On an overseas mission, the attorney, a naturalized U.S. citizen fluent in a foreign language, suddenly lost access to an American compound based on a "country clearance"

[99] *See* 5 C.F.R. § 9901.512, https://www.govinfo.gov/content/pkg/CFR-2011-title5-vol3/xml/CFR-2011-title5-vol3-sec9901-512.xml. Interview with Anonymous Whistleblower (Apr. 15, 2021).
[100] Interview with Anonymous Whistleblower (June 16, 2021).

issue.[101] ITMS officials purportedly learned about a sanctioned interaction between a high-ranking foreign government official and the attorney during a meeting approved by the U.S. Embassy before launching a security investigation. Once the attorney returned stateside, ITMS conducted multiple interrogations in what whistleblowers described as a "fishing expedition." Agents did not advise the attorney of legal rights during these interrogations or disclose the reason for their investigation. The unit searched the attorney's emails as well. Although the Department never accused the attorney of wrongdoing, the investigation caused irreparable professional damage. Nearly a decade later, the attorney has not received any subsequent pay grade increases on the federal civilian employee scale.

In addition, whistleblowers claimed that some cases are opened for the sole purpose of intimidation. In one case, a senior ITMS official discussed an investigation into a Department employee who reported a stolen Personal Identity Verification (PIV) card. Officials chose not to refer the matter to a law enforcement agency for further investigation. Instead of closing the case, however, the official said, "I wouldn't necessarily say the case is closed, but I don't anticipate any further investigative activity on our part."[102] This practice of leaving cases open became part of a pattern used by ITMS to harm the subject's internal promotion prospects, as well as external employment possibilities within the federal government, based upon the unit's determination that the individual posed a security threat.

Key Findings

The ITMS targeted employees for investigation within the ITMS for challenging the unit's legal authorities, demonstrating an egregious pattern of reprisal. Across the Department, the ITMS opened investigations into a variety of employees without reasonable suspicion for the purpose of exaggerating the unit's ability to uncover security threats within the civil service. Expanding the unit's power became the modus operandi, which led ITMS officials to target any individual who stood in the way.

F. FUNDING AND WASTE

The Department of Commerce funded the Investigations and Threat Management Service (ITMS) through the Working Capital Fund (WCF) for most of the unit's existence. This means that the ITMS largely operated with minimal oversight from the congressional appropriations process, resulting in gross waste across the Department as frivolous investigations suspended operations in entire component offices and case backlogs developed.

Working Capital Fund

Use of the Working Capital Fund played a key role in shielding ITMS activities from congressional oversight for most of the unit's existence. The ITMS, and its earlier iterations, primarily received

[101] Interview with Anonymous Whistleblower (Apr. 19, 2021).
[102] Email from Thomas Valentine, Investigations and Threat Mgmt. Serv., to William Bent (Dec. 17, 2020), https://www.commerce.senate.gov/services/files/7F85FBCD-446C-4798-AC5A-9237DFC79F47.

funding as part of Office of Security (OSY) from the WCF.[103] This discretionary account dates back to the 1940s, and has been used historically to provide bureaus with added administrative support to accomplish the Department's overall mission.[104] It operates as a revolving slush fund–– without receiving regular appropriations—which provides broad opportunity for abuse to component divisions whose operations depend on it for resources.

Congressional Appropriations

In addition, the Department has requested funding for the unit from Congress periodically through the Office of Security since the Obama administration. The Department described the unit, which first appeared as the Investigations and Intelligence Program, as having a counterintelligence mission each year that it submitted a budget request for its activities under that name, as well as under the Investigations and Intelligence Division, the Investigations and Threat Management Division, and most recently as the Investigations and Threat Management Service. At no point, however, did the ITMS properly maintain authorization to engage in counterintelligence activities.

In the Budget Justification for Fiscal Year 2011, for example, the Department argued:

> Mission critical threats emanate from foreign intelligence services, sophisticated criminal organizations, and violent extremists whose actions impact Departmental personal, assets, and activities in furtherance of their own economic, technological, or environmental agendas. The Office of Security is the only operating unit specifically chartered to protect the Department from these type of threats, as well as the only governmental entity functioning in this capacity that is directly focused on the Department.[105]

After receiving appropriations for these purposes, the unit significantly broadened its involvement in activities usually reserved for actors in the Intelligence Community. The gradual growth of the unit's capabilities even led the Department to declare in the Budget Justification for Fiscal Year 2018 that it filled objectives related to "counterintelligence, transnational organized crime, and counterterrorism." Despite lacking clearly defined authority to collaborate with agencies in the Intelligence Community, the Department claimed that the unit "directly inform[ed] key decision-makers and stakeholders about threats to national security,"[106] including officials at the Cabinet-Secretary level in the Office of the Director of National Intelligence and at the Department of Justice. The Budget Justification even claimed the ITMS assisted with the National Security Strategy, a periodic document released by the President to detail the administration's interagency approach for addressing threats to national security.[107]

In the Budget Justification for Fiscal Year 2021, the ITMS sought to complete its evolution into a proxy spy unit operating outside the Intelligence Community. The Department requested funds, in

---

[103] *Supra* note 44. The Management Division of the Department of Commerce receives funding through the Salaries and Expense appropriation (S&E) and the Working Capital Fund.
[104] https://www.commerce.gov/sites/default/files/2021-03/DM_FY_2021_Final_WCF_and_AR_Handbook.pdf
[105] *Supra* note 44.
[106] *Supra* note 42. (Parenthesis omitted).
[107] *Id*.

particular, so the ITMS could continue "safeguarding classified, sensitive documents" using an encrypted database.[108] Officials requested funds to procure Authentic8 Silo Toolbox, which describes itself as "an integrated platform for conducting web research without exposing [the user's] digital signature." The company purports to assist government agencies with intelligence and evidence gathering, as well as undercover operations, by providing a "global cloud-based infrastructure" for controlling multifaceted databases.[109] It is not clear whether the unit ultimately obtained funding for this purpose, but whistleblowers claim that officials continue to use Microsoft Excel spreadsheets for case management.

Waste

Congress has approved millions of dollars in appropriations to the Department of Commerce Working Capital Fund, which has allowed the ITMS to pursue an unauthorized mission largely out of sight from the appropriations process. As a practical effect, almost two-thousand cases reportedly remained open at the end of 2020. This suggests an overbroad characterization of what constituted a "mission critical threat" and "critical asset," practices that allowed the ITMS to investigate matters outside of its jurisdiction.

Recent appropriations also qualify as a waste of taxpayer dollars because departmental officials misled Congress about the unit's reorganization and need for additional criminal investigators. In this sense, the Department said in a recent Budget Justification that it sought a significant funding increase "to address critical staffing shortfalls commensurate with workload demands from previous expansions that were never fully implemented."[110] The Department argued that "ongoing and anticipated casework is expected to directly decrease the ability of hostile intelligence services to exploit Departmental policy [and] research" and "decrease the ability of organized crime figures to divert Departmental objectives."[111] Officials also claimed that

> Based on historical data, it is estimated that 5.1% of ITM[S]'s intakes and inquiries have become full investigations, which leaves up to 23 potentially high risk matters presently in inventory that have yet to be fully addressed. Of 31 investigative matters that are or could be high risk to the Department, ITM[S] currently has sufficient staff to fully investigate only 6 cases, which leaves 81% not being worked in a timely manner after initial triage. Based on previously uncovered matters, these threats are anticipated to have a direct impact to the Department's major strategic interests.[112]

Rather than insufficient resources causing the case backlog, agents described the processes used by ITMS to investigate threats as "convoluted" and "dysfunctional."[113] Whistleblowers claimed that senior officials even refused to assign matters that escalated into investigations for agents to pursue, slowing the rate agents evaluated potential threats.

---

[108] FY 2021 Congressional Submission, *available at* https://www.commerce.gov/sites/default/files/2020-02/fy2021_dm_congressional_budget_justification.pdf
[109] Authentic8, *Why Silo*, available at https://www.authentic8.com/why-silo.
[110] *Supra* note 42.
[111] *Id*.
[112] *Id*.
[113] *Supra* note 87.

In addition, most opened cases reportedly lacked due diligence for extended periods of time. According to Supervisory Special Agent Clifton Dyer in a memo dated August 2020, "[t]here are some inquiries in this office that have been open for up to seven years with little to no investigative action taken."[114] As a result, "the average number of days an intake has been open without any investigative activity or supervisory guidance is 690," or nearly two years.[115] Dyer explained that many opened cases focused on non-threatening communications to the Department from federal inmates seeking open source information, such as how to obtain a patent. Dyer said there was "no reason to have 90% of these cases opened," but predicted that senior ITMS officials sought to maintain a high number of opened cases in order to inflate the unit's ability to assess threats and conduct wide-ranging investigations.[116]

For the duration of the unit's existence, baseless investigations caused gross waste across the Department. After the ITMS began investigating the entire staff of the Office of Executive Security (OES) for security violations, the employees "were sequestered to different conference rooms within the Herbert C. Hoover Building . . . without any duties" for an extended period of time.[117] The ITMS purportedly initiated these investigations to sideline the office as means of obtaining a direct line to the Intelligence Community. According to a report from OIG, an ITMS official even monitored the employees for some time in a conference room, and eventually, employees resorted to watching Netflix, playing on their personal phones, and even made "Gummy Bear art" on duty.[118] Despite the suspension of duties during this period, the Department used $1,179,154 in taxpayer dollars to pay the sidelined OES employees for a "collective total of 127 months."[119] Ultimately, the ITMS referred three employees to the Department of Justice for prosecution, but all referrals were declined. Whistleblowers confirmed that the allegations against OES personnel were unsubstantiated, meaning that disbursement of salaries for the OES employees baselessly suspended amounted to gross waste.

The ITMS even opened a "protective intelligence" investigation after the Department received a harmless communication from elementary school children.[120] One child sent a petition to the Secretary of Commerce, along with multiple classmates as cosignatories, requesting the addition of a certain type of whale to the list of protected marine wildlife in the Marine Mammal Protection Act of 1972. To any reasonable observer, the letter posed no threat to the Department. The ITMS, nonetheless, not only opened a case but conducted a search of the author's name—a minor—in government databases like the FBI's National Crime Information Center (NCIC) and the Department of Homeland Security's Targeted Violence Information Sharing System (TAVISS).

---

[114] *Id*.
[115] *Id*.
[116] *Id*.
[117] Office of the Inspector Gen., Dep't of Commerce, 19-0108, *OSY Investigation of [OES]*, 1 (Jun. 23, 2020), https://www.oig.doc.gov/OIGPublications/ROI-19-0108%20-%20Redacted%20Appeal%202021-001240.pdf
[118] *Id*. at 5.
[119] *Id*. at 9.
[120] Email from Clifton Dyer, Supervisory Special Agent, Dep't of Commerce, to Minority Committee Staff (June 30, 2021), https://www.commerce.senate.gov/services/files/7F85FBCD-446C-4798-AC5A-9237DFC79F47.

Key Findings

The Department used the Working Capital Fund to supply the ITMS with the resources it needed to conduct criminal and counterintelligence investigations largely out of sight from the congressional appropriations process. This allowed the unit to operate with minimal accountability and sustain a mission irreconcilable with its intended purpose of providing protective security services.

G. OVERSIGHT FROM THE OFFICE OF THE INSPECTOR GENERAL

The Inspector General Act of 1978 established the Office of Inspector General at the Department of Commerce (OIG).[121] Congress intended the Inspector General to serve as an "independent and objective unit" to "promote economy, efficiency, and effectiveness" and "prevent and detect fraud and abuse" at the Department.[122] The Act also contemplated that Inspectors General would keep "Congress fully and currently informed about problems and deficiencies relating to the administration of such programs and operations and the necessity for and progress of corrective actions."[123] Unfortunately, the OIG failed to notify Congress about abuses at the ITMS after investigating claims of misconduct as far back as 2017.

Overview

The Office of Inspector General at the Department of Commerce (OIG), which is tasked with investigating and auditing waste, fraud, and abuse, has long suffered from chronic mismanagement. In the last sixteen years, five separate Inspectors General have served at the Department with tenures punctuated by public scandal and underperformance.[124] This investigation revealed that the office, under the leadership of Inspector General Peggy Gustafson, has failed to identify wide-ranging abuses within the Investigations and Threat Management Service (ITMS).

On multiple occasions, the OIG probed whether the unit abused the Special Deputation program from the U.S. Marshals Service, whether it had authority to conduct counterintelligence investigations, and whether it targeted individuals of Asian ancestry. Ranking Member Wicker requested the reports detailing these investigations. Instead of voluntarily disclosing them to the Committee, the OIG processed the request under the Freedom of Information Act (FOIA, citing an advisory opinion from the Justice Department that effectively authorizes agencies to ignore oversight requests from Ranking Members.[125] In the end, OIG then released only a portion of

---

[121] Pub. L. 95–452, §1, Oct. 12, 1978, 92 Stat. 1101 (1978), as amended, *codified at* 5 U.S.C. App. §§ 1-13 (IG Act)
[122] *Id*.
[123] 5 U.S.C. App. (IG Act) §2.
[124] The most recent two Senate-confirmed IGs resigned amid allegations of fraud and whistleblower retaliation. *See* Colby Itkowitz, *Embattled Commerce IG Todd Zinser Steps Down*, WASH. POST. (June 4, 2015), https://www.washingtonpost.com/blogs/in-the-loop/wp/2015/06/04/embattled-commerce-ig-todd-zinser-steps-down/, *Commerce Department Inspector General Resigns Amid Ethics Probe*, FOX NEWS (June 8, 2007), https://www.foxnews.com/story/commerce-department-inspector-general-resigns-amid-ethics-probe.
[125] *See* Authority of Individual Members of Congress to Conduct Oversight of the Executive Branch, 41 Op. O.L.C. (2017) (allowing agencies to ignore document requests from Ranking Members of congressional committees); Letter from Peggy Gustafson, Inspector Gen., Dep't of Commerce, to Ranking Member Roger Wicker, S. Comm. on

documents responsive to this request, citing FOIA exemptions that permit agencies to withhold files under the Privacy Act.[126]

Investigations

As far back as 2017, the office investigated the scope of the unit's law enforcement authorities without offering detailed conclusions about the reported abuse of power.[127] The watchdog conducted its first known probe after receiving concerns in May 2017 from the U.S. Marshals Service about the unit's use of Special Deputations for improper purposes. Even though the complaint accused the ITMS of misusing Special Deputations by "conduct[ing] investigations," the OIG concluded that its "preliminary investigation generally unsubstantiated the allegations."[128] The OIG noted, however, that "the listing of ITM[S] agents solely as Protection Detail personnel" on the Special Deputation application "could be problematic to their mission."[129] The report offered no further recommendations.

The same report raised concerns about whether the unit had the authority to conduct counterintelligence operations. It noted that the Office of Security should "seek clarification from the Office of the Director of National Intelligence on ITM[S]' authority and possible need to affiliate with the Intelligence Community."[130] No discussion on this subject took place in response between the ITMS and ODNI as a subsequent communication with OIG memorialized.

Not until late 2018 did the OIG request a more complete review of the unit's affiliation with the Intelligence Community after the Department described its mission in a submission to Congress as focused on counterintelligence. The OIG sought to evaluate the scope of legal authorities allowing ITMS to exercise counterintelligence tools. In response, the unit described itself generally as a law enforcement agency and admitted that it "associates, cooperates, and consults" with members of the Intelligence Community, even though the Commerce Department is not officially a member.[131]

This answer prompted OIG to request a supplementary response focusing on the nature of the relationship between ITMS and intelligence agencies.[132] The ITMS acknowledged that it filled the role of Federal Senior Intelligence Coordinator for the Commerce Department, meaning it served as the direct line to the Intelligence Community regarding the Department's role in combatting threats to national security related to insider threats, cybersecurity, and counterterrorism.[133] The

---

Commerce, Sci., and Transp. (March 19, 2021), https://www.commerce.senate.gov/services/files/2F09349F-6461-4185-A7C6-EC77ABE1BB2D.

[126] *See* Application of Privacy Act Congressional-Disclosure Exception to Disclosures to Ranking Minority Members, 25 Op. O.L.C. 289, 289 (2001).

[127] Office of the Inspector Gen., Dep't of Commerce, *Referral from USMS to Department of Commerce Office of Inspector General*, 1 (2017), https://www.commerce.senate.gov/services/files/640BDA8F-A7F0-483C-B541-C1F75DABDE5D.

[128] *Id*. at 1.

[129] *Id*. at 2.

[130] *Id*. at 3.

[131] *Supra* note 23.

[132] Memorandum from Peggy Gustafson, Inspector Gen., Dep't of Commerce (Feb. 19, 2019), https://www.commerce.senate.gov/services/files/640BDA8F-A7F0-483C-B541-C1F75DABDE5D.

[133] *Supra* note 49.

ITMS also detailed the reviews of its counterintelligence program by the Office of the National Counterintelligence Executive, a component of the Office of the Director of National Intelligence, to justify its continued involvement in counterintelligence operations.[134]

These reviews, along with vague statements about the unit's activities from Director of Security Richard Townsend, led the OIG to conclude in mid-2019 that the ITMS "does not originate investigative activities solely with the intent of engaging in counterintelligence, and does not engage unilaterally in traditional U.S. Intelligence Community counterintelligence operations."[135] The OIG noted that it found explanations of references to "counterintelligence" from Director Townsend in public mission statements and internal documents "generally useful in clarifying the role of the ITM[S]."[136]

To close out the matter, the OIG recommended only that the Department strike reference to "counterintelligence" in the Departmental Administrative Order (DAO) 207-11 detailing the scope of authorities in the Official Credential and Badge section of the Security Manuel and the DAO describing the mission of the ITMS within the Office of Security.[137] The ITMS claimed it intended to work with departmental partners to comply. As of July 2021, the Department had not made these changes.

In addition, the OIG investigated at least one referral from the U.S. Marshals Service in 2017 concerning the ITMS targeting "persons primarily of a particular ancestry."[138] The complaint described ITMS cases involving the "possible recruitment by a certain country's government of U.S.-based persons with ancestry from that country," and noted as a result that "subjects [were] likely to be of a certain ancestry."[139] This description likely suggests that Chinese-Americans formed the basis of this complaint since the Department has acknowledged it views the Chinese government as threatening to global economic and national security interests. The OIG noted that its investigators with knowledge of these cases unrelated to this probe found "no reason to believe racial, ethnic, or cultural bias [was] a motivator."[140] It appears that OIG did not otherwise investigate this claim.

As the Minority Staff investigation unfolded, whistleblowers reported that the OIG began investigating multiple allegations of misconduct into leading officials within the Office of Security, including George Lee, Richard Townsend, and Thomas Valentine. Those investigations are ongoing matters.

---

[134] *Id*.
[135] Memorandum from Peggy Gustafson, Inspector Gen., Dep't of Commerce, to Wilbur Ross, Sec'y, Dep't of Commerce (June 7, 2019), https://www.commerce.senate.gov/services/files/640BDA8F-A7F0-483C-B541-C1F75DABDE5D.
[136] *Id*.
[137] *Id*.
[138] *Supra* note 127, at 1.
[139] *Id*. at 2.
[140] *Id*.

Key Findings

Based on the reports produced to Minority Staff, past OIG investigations lacked the veracity to identify and resolve the unlawful conduct that has plagued the ITMS for more than a decade. An OIG official even told Minority Staff that the office's investigations "satisfied" internal requirements but likely were "not satisfactory" on the merits.[141]

Without proper functioning of the safeguard Congress put in place to identify waste, fraud, and abuse when it passed the Inspector General Act of 1978, the ITMS operated largely in the shadows across multiple administrations. Because of inadequate oversight by the Inspector General's office, the unit's improper exercises of law enforcement powers likely resulted in preventable violations of civil liberties and other constitutional rights, as well as a gross abuse of taxpayer funds.

VI. CONCLUSION

For sixteen years, the Investigations and Threat Management Service operated within the Department of Commerce without proper authority or meaningful oversight. The unit regularly disregarded the rule of law, committing gross abuses of power and misusing taxpayer funds to perform missions the unit lacked authorization to undertake. Although the misconduct spanned multiple presidential administrations, the Executive Branch only acknowledged that the unit had operated largely in the shadows with the appointment of John Costello as Deputy Assistant Secretary for Intelligence and Security in 2020.

The Department of Commerce plays a vital role in the economic prosperity and national security of the United States. Identifying and mitigating risks to these objectives should be a priority for the federal government. Divisions like the Investigations and Threat Management Service tasked with risk-mitigation missions, however, must safeguard key interests in compliance with regulatory, statutory, and constitutional law.

As whistleblowers provided detailed and consistent accounts of misconduct, Ranking Member Wicker sent a letter to Secretary of Commerce Gina Raimondo on April 27, 2021, to provide notification about the investigation and request cooperation regarding access to additional witnesses and documents.[142] In response to Ranking Member Wicker's letter, the Department issued a temporary order requiring that ITMS cease investigative activities on May 14, 2021, and pledged to "implement a comprehensive solution to the issues raised."[143] Subsequent dialogue with Department of Commerce officials resulted in access to additional documents and witness testimony, which helped this Committee perform its oversight role.

Congress has a well-defined constitutional interest in performing oversight of the Executive Branch, which requires access to documents and testimony for accountability. At the same time,

[141] Video Interview with Anonymous Official, Office of the Inspector Gen., Dep't of Commerce (Apr. 15. 2021).
[142] Letter from Sen. Roger Wicker, Ranking Member, S. Comm. on Commerce, Sci., and Transp., to Gina Raimondo, Sec'y, Dep't of Commerce (Apr. 27, 2021), https://www.commerce.senate.gov/services/files/2F09349F-6461-4185-A7C6-EC77ABE1BB2D.
[143] Letter from the Dep't of Commerce to Sen. Roger Wicker, Ranking Member, S. Comm. on Commerce, Sci., and Transp. (May 14, 2021), https://www.commerce.senate.gov/services/files/2F09349F-6461-4185-A7C6-EC77ABE1BB2D.

Congress established Inspectors General to discover waste, fraud, and abuse—including certain types of criminal activity—within federal departments before the misconduct rises to a level of congressional concern. Under the deficient leadership of Inspector General Peggy Gustafson, the ITMS abused its power, discriminately targeted Department employees, and wasted taxpayer funds performing an unauthorized mission. These activities continued for an extended period of time, despite the Inspector General's awareness of the unit's structural and operational defects.

VII. RECOMMENDATIONS

The Committee remains diligent in its oversight of the Department of Commerce, and Ranking Member Wicker is committed to working with officials on implementing corrective actions targeted at the Investigations and Threat Management Service (ITMS). After reviewing thousands of documents and conducting interviews with more than two dozen whistleblowers and Department officials, Minority Staff recommend the following actions:

- The Department of Commerce should evaluate the future of the ITMS, including possible structural reforms to ensure better oversight and potential legislation to authorize legitimate aspects of the unit's investigative mission.

- The Department of Commerce should conduct an administrative and legal review of ITMS policies and procedures to ensure compliance with statutes, regulations, and professional standards.

- The Department of Commerce should conduct a review of all adverse employment actions directed or informed by the work of ITMS and former iterations of the office. The review should include, but not be limited to, disciplinary matters; suspension or revocation of security clearances; and retirements, resignations, and terminations. Significant scrutiny should be placed on related Non-Disclosure, Resolution, Settlement, and other agreements negotiated by ITMS officials, including George Lee.

- The administration should conduct an administrative and legal review of closed ITMS cases, including potential referral of criminal misconduct to the appropriate prosecutorial authorities.

- The Department of Justice should conduct a thorough review of policies and procedures governing the Special Deputation program to improve oversight and prevent future abuses.