OFFICE OF INSPECTOR GENERAL
OFFICE OF INVESTIGATIONS

REPORT OF INVESTIGATION

CASE TITLE:	FILE NO.:
[redacted] (OS/ITMD)	19-0714
	TYPE OF REPORT: ☐ Interim ☒ Final ☐ Supplemental

BASIS FOR INVESTIGATION

In July 2019, the U.S. Department of Commerce (Department), Office of Inspector General (OIG) received an initial complaint regarding [redacted] (Subject), [redacted] Investigations and Threat Management Section (ITMS), for targeting ITMS employees and conducting inappropriate office searches of Department employees. Investigative steps led to additional allegations. The allegations are:

1. Subject violated Department policy directing non-consensual audio recordings.
2. Subject carelessly handled badge and credentials for a former ITMS employee in violation of DAO 207-11, section 7.09.
3. Subject requested e-mails between former employee and OIG personnel.
4. Subject abused [redacted] position of authority with [redacted] Office of Enforcement Analysis (OEA), Bureau of Industry and Security (BIS).
5. OSY inappropriately directed the suspensions of security clearances of two NIST [redacted] for arranging an unclassified briefing against the wishes of subject and [redacted] OSY.
6. Subject misused government resources by directing ITMS personnel to transport [redacted] for personal travel in a government vehicle.
7. Subject improperly obtained a Unique Flying Armed Number (UFAN) and ITMS has operated without a flying armed policy since [redacted]
8. Subject created a toxic work environment.

Distr bution:	OS
Signature of Case Agent [redacted]	Signature [redacted] Approving Official

9. Subject did not follow security manager protocol.
10. Inappropriate basis for United States Marshals Service (USMS) deputation for ITMS.
11. ITMS failed to afford the appropriate rights, warnings, or expectations of privacy to interviewees and searches of department employees.
12. Subject routinely pulled employees' e-mail to see if they violated non-disclosure agreements (NDAs).
13. Subject directed inappropriate searches of Department employees' office spaces.
14. Subject directed alteration of documents.
15. Subject committed travel fraud to [redacted] Virginia.

SUMMARY OF INVESTIGATIVE FINDINGS

INVESTIGATIVE METHODOLOGY

OIG conducted interviews of ITMS and Department employees and the Subject. OIG reviewed travel orders, e-mails, ITMS case files, ITMS case management system (CNET), and conducted an administrative search of the Subject's office.

DETAILS OF INVESTIGATION AND FINDINGS

OIG's findings regarding the allegations raised in this case are set forth below along with supporting evidence.

1. *Allegation: Subject Violated Department Policy by Directing Non-Consensual Audio Recordings*

Department Administrative Order (DAO) 207-9, section 2 provides that "under no circumstances shall a Department officer or employee in the course of his official duties use electronic or mechanical devices secretly to overhear, transmit or record telephonic and oral non-telephonic communications." Section 4 of that DAO does contain an exception to that prohibition that permits law enforcement within the Department to monitor conversations "with the concurrence of the appropriate legal counsel":

> The prohibitions of this Order shall be inapplicable to monitoring conducted in the course of bona fide law enforcement activities of the Department's various law enforcement offices, to wit: the Office of Security…as long as the activities that would otherwise be prohibited by this Order are

> specifically authorized by the head of the operating unit (as defined in DOO 1-1, "Mission and Organization of the Department of Commerce") for the office engaged in such activities, with the concurrence of the appropriate legal counsel, and are conducted pursuant to and in accordance with all applicable federal laws, regulations, and Attorney General Guidelines.[1]

Subject was interviewed and said ITMS does not have a policy regarding covert recordings, but they do follow DAO 207-9. Three senior attorneys within OGC who [redacted] its employment law responsibilities —[redacted], and [redacted] —related the Subject never discussed conducting non-consensual recordings with them; and they never provided guidance regarding non-consensual recordings conducted for an interview in [redacted] or a meeting for the "[redacted]" case discussed below, as the DAO requires.

[redacted] Interview

[redacted] (SA 1), [redacted] Special Agent, ITMS, related sometime around mid-[redacted] and Subject went to [redacted] to conduct a witness interview for an investigation. SA 1 said Subject instructed [redacted] to covertly record the interview because Subject was afraid the witness's attorney would cancel the interview if they knew it was being recorded. SA 1 placed a digital recording device in a closed portfolio on the table during the interview and turned it over to Subject after the interview.

Subject was interviewed and affirmed [redacted] instructed SA 1 to covertly record the interview. Subject confirmed legal counsel was not consulted prior to this covert recording because it was last minute, (although the trip to [redacted] to conduct the interview was pre-planned). Subject could not explain why the interview could not be recorded with consent from the witness.

OIG determined Subject violated Department policy by directing a non-consensual audio recording without concurrence of the appropriate legal counsel. OGC affirmed Subject did not consult with them. Subject stated the interview was last minute; however, it was a planned trip for the purpose of conducting the interview and Subject purposely covertly recorded the interview for fear the interviewee's attorney would cancel it.

---

[1] U.S. Department of Commerce. *Department Administrative Order 207-9* [online]. www.osec.doc.gov/opog/dmp/daos/dao207_9.html (accessed December 29, 2020).

[redacted] Investigation

SA 1 said in [redacted], during an investigation of the [redacted], Subject instructed [redacted] to record a technical meeting attended by 12 Department employees and contractors at a [redacted] location in [redacted] MD. SA 1 said Subject did not explicitly say to record it overtly or covertly, but SA 1 felt pressure from Subject to get the recording done and worried about ramifications if [redacted] did not get the recording. SA 1 placed a digital recording device in an open portfolio on the table during the meeting and covertly recorded the meeting without the knowledge of other participants. SA 1 said [redacted] subsequently provided the recording to Subject. SA 1 said after the recorded meeting there was a debriefing at the Herbert C. Hoover Building, Washington, DC, where a disagreement between Subject and the [redacted] for the Office of the Secretary ensued. SA 1 related Subject announced that there was a recording of the meeting, as if it was an "Aha! I have you on recording!"

[redacted] (SA 2), Special Agent, ITMS, witnessed Subject tell SA 1 to record the meeting and had the impression it was to be recorded "one way or another." SA 2 described Subject's directive as very awkward and "not feel[ing] right." SA 1 commented to SA 2, "I don't know if I like that." SA 1 contacted SA 2 several times with [redacted] uneasiness.

Subject said [redacted] told SA 1 to record the meeting overtly.

Based on the information above, Subject did not violate DAO 207-9 because [redacted] did not direct a covert recording and accordingly, [redacted] did not need to obtain concurrence of the appropriate legal counsel.

2. *Allegation: Subject Carelessly Handled Badge and Credentials for a Former ITMS Employee in Violation of DAO 207-11, Section 7.09*

DAO 207-11, Section 7.09 states, "The careless handling, abuse, misuse, or intentional misrepresentation of official credentials and badges shall be cause for possible administrative or disciplinary action."

During OIG's administrative search of Subject's office, Department Badge [redacted] and credentials (DOC OSY [redacted]) for [redacted] (SA 3), former Special Agent, ITMS, were found in the top cabinet behind Subject's desk. They were discovered among piles of disorganized and haphazardly-placed papers, notebooks, and media. Inquiries with OSY revealed the badge and credentials were reported lost by [redacted] ITMS. According to the report, the badge and

credentials were received in the mail by [redacted] and held in an ITMS locked file cabinet pending SA 3's separation from service.

Subject was interviewed and related [redacted] never saw SA 3's badge and credentials and did not know they were missing.

Subject stated in [redacted] interview to OIG that [redacted] had no knowledge of the whereabouts of the badge and credentials that were found in [redacted] locked office. OIG's administrative search and accompanying investigation indicated the badge and credentials were possibly in Subject's office for approximately 3 years (date of report of missing badge and credentials filed by SA 3[redacted] on [redacted]), a space where others did not have general access. The discovery of the missing badge and credentials in Subject's office indicates Subject carelessly handled the badge and credentials, and [redacted] should have returned them to OSY, as is the proper protocol when a law enforcement official leaves the Department, all in violation of DAO 207-11, Section 7.09.

3. *Allegation: Subject Requested E-mails Between Former Employee and OIG Personnel*

A review of Subject's e-mails showed correspondence between Subject and the Department's Office of Privacy and Open Government (Privacy Office) in [redacted] wherein Subject requested e-mails between a former ITMS special agent (Former Employee) and two OIG Office of Investigations special agents (OI Special Agents). Subject said [redacted] needed to view e-mails pertaining to "ongoing investigations of threats involving forty or more individuals" because [redacted] was not carbon copied when they were originally sent. Subject noted [redacted] received the e-mails, then requested e-mails between Former Employee and OI Special Agents and "anyone in OIG."

Several individuals within the Privacy Office were interviewed and provided an e-mail chain involving OSY, Information Technology (IT), and OGC wherein IT requested an official reason to pull the e-mails. Subject replied, "The official reason for requesting the e-mail is that as a supervisor I need the work product it contains. There is no investigation, [Office of Human Resources (OHR)], [Inspector General (IG)], OGC, or other matters." IT requested assistance from OGC.

[redacted] OGC, provided that Subject indicated [redacted] request was not for an official investigation, but to obtain e-mails for which [redacted] was not carbon copied. [redacted] believed Subject's request was not appropriate—within the principles of privacy rights, expectations, and norms—to obtain unfettered access to an employee's e-mail. [redacted] thought Subject should be able to identify specific search terms. [redacted] suspicioned the request was actually for an official investigation based on how "that office operates." [redacted] speculated [redacted] supervisor, [redacted]

[redacted] (Supervisor), spoke directly with Subject and then directed [redacted] to respond to OES that (B)(5) Withholding at Department Request [redacted]. [redacted] did not know the reason for [redacted]. [redacted] did not know what Subject's purpose was for the e-mails between Former Employee and OIG. [redacted] said that if [redacted] had known the request was for e-mails between Former Employee and OIG, [redacted] might have had concerns about potential abuse by Subject or action against a potential whistleblower. [redacted] believed Supervisor spoke with Subject about justification for this request.

Supervisor was interviewed and related [redacted] had many conversations with Subject about pulling e-mails, but does not recall an instance wherein Subject wanted e-mails between Former Employee and OI Special Agents. Supervisor said [redacted] would likely remember that type of request.

[redacted] OSY, and Supervisor did not have any knowledge that Subject pulled e-mails between Former Employee and OIG personnel.

Subject was interviewed and related [redacted] did request and receive all of the above e-mails to assist with reassignment of the investigative cases connected to ongoing investigations for "a specific threat involving multiple individuals."

Title 5 U.S.C. § 2302(b)(8)(A)(i-ii), protects federal employees from retaliation for disclosing to the Inspector General information he reasonably believes evidences "any violation … of any law, rule, or regulation, or gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to the public health or safety." OIG was not able to determine Subject's motivation for this email request; however, it is important for an agency to avoid a situation where employees believe their communications with OIG are being monitored.

Subject could have obtained these emails in other ways. We note that Subject could have asked Former Employee for the information prior to Former Employee's [redacted]. Subject could have asked OIG for the information. Also of note, the investigations Subject referenced as justification for pulling the e-mails were either being worked jointly between ITMS and OIG or had been referred to OIG. Many of the witnesses interviewed did not know all of the details of Subject's request, but assisted in the request assuming others had vetted it.

4. *Allegation: Subject Abused [redacted] Position of Authority with [redacted], OEA, BIS*

Chapter 5 C.F.R. § 2635.704(a) provides the standard that "[a]n employee has a duty to protect and conserve Government property and shall not use such property, or allow its use, for other than authorized purposes."

Chapter 5 C.F.R. § 2635.101(b) provides general principles that apply to every employee. Subsection (b)(9) of this section states that "[e]mployees shall protect and conserve Federal property and shall not use it for other than authorized activities." Subsection (b)(14) of the same section states that "[e]mployees shall endeavor to avoid any actions creating the appearance that they are violating the law or the ethical standards set forth in this part. Whether particular circumstances create an appearance that the law or these standards have been violated shall be determined from the perspective of a reasonable person with knowledge of the facts."

DAO 207-11, Section 7.01 states, "[t]he Form CD-277 [credentials] and badge shall be used only for official law enforcement, investigation, and liaison duties and not for transacting personal or non-official business or for any purpose other than specified in this Order."

[redacted] (SA 4), [redacted] Special Agent, ITMS, related sometime between [redacted], Subject informed [redacted] was asked to leave a meeting with [redacted] OEA, BIS, and [redacted] OSY, at the time and [redacted] Subject directed SA 4 to help [redacted] interview [redacted] OEA to find out what occurred in the meeting after Subject left. SA 4 related Subject read the "first two lines" of 18 U.S.C. § 1001, False Statements, to [redacted] OEA and explained it was criminal to lie to a federal law enforcement officer. SA 4 said Subject displayed [redacted] credentials in an unprofessional manner, close to [redacted] OEA's face, was confrontational, and demanded to know what was discussed in the meeting after [redacted] was asked to step out.

[redacted] OEA affirmed Subject was asked to leave the meeting by [redacted] OSY and Subject subsequently confronted [redacted] OEA. [redacted] OEA confirmed Subject displayed [redacted] law enforcement badge and credentials and demanded to know what was discussed in the meeting after [redacted] was told to leave. [redacted] OEA could not remember if Subject cited false statements to a law enforcement officer as a criminal offense, but said Subject's actions were inappropriate and felt that Subject abused [redacted] position as a law enforcement officer to pressure or bully [redacted] into relating what was discussed in the meeting after Subject was excused, especially since it was likely not for law enforcement purposes. Subject also instructed [redacted] OEA not to discuss an investigation into the [redacted] with anyone other than Subject, to include

Subject's supervisors. [redacted] OEA felt Subject's supervisors were not able to manage Subject and said Subject exuded an "I'm in control" attitude.

Subject was interviewed and admitted to being asked to leave the meeting. Subject said [redacted] took SA 4 with [redacted] to confront [redacted] OEA about what transpired in the meeting after [redacted] left. Subject did not recall if [redacted] displayed [redacted] law enforcement credentials or if [redacted] cited 18 U.S.C. § 1001. Subject affirmed [redacted] instructed [redacted] OEA not to discuss the [redacted] investigation with Subject's supervisors and only with [redacted] [redacted] OEA felt this demand was a control tactic because Subject felt [redacted] was in charge.

5. *Allegation: OSY Inappropriately Directed the Suspensions of Security Clearances of Two NIST [redacted] for Arranging an Unclassified Briefing Against the Wishes of Subject and [redacted] OSY*

Interviews with [redacted] NIST; [redacted], NIST; their [redacted] and other NIST personnel revealed NIST tried to coordinate a briefing on possible threats of foreign researchers to NIST laboratory leadership through [redacted] OSY as early as the end of [redacted]. Neither Subject nor [redacted] OSY coordinated the briefing, so in [redacted] scheduled an unclassified briefing through the FBI. NIST leadership felt this training was important to boost awareness for and help prevent foreign talent recruitment.

[redacted] was told by [redacted] OSY and Subject to stand down on having the briefing without providing a reason. [redacted] said they cited a policy which they claimed dictated that [redacted] heed their order to cancel the briefing. [redacted] did not know what the policy was. [redacted] replied [redacted] would stand down if told by [redacted] NIST. [redacted] felt Subject was irritated and that [redacted] needed "to be taught a lesson" for not acquiescing to their order.

[redacted] and [redacted] postponed the FBI briefing for 30 days to afford OSY time to provide the briefing, but OSY did not provide the briefing within this 30-day period, so they rescheduled it for [redacted]. Approximately a week after the briefing was held, both [redacted] security clearances were suspended by [redacted] InfoSec at the direction of [redacted] OSY. [redacted] and [redacted] did not have their secret and top-secret clearances reinstated for almost [redacted] months after they were suspended, which caused NIST to scramble to find others to attend classified briefings and precluded [redacted] and [redacted] from being able to conduct their jobs. As of the date of this report, [redacted] and never had [redacted] Sensitive Compartmented Information

(SCI) reinstated. [redacted] still does not have [redacted] SCI clearance, which is more than [redacted] after it was suspended.

Following the suspensions, a security clearance investigation was conducted by InfoSec. The investigators interviewed [redacted] and [redacted] and concluded they disobeyed an order. However, neither investigator knew the briefing was unclassified. One investigator opined the security suspension seemed "heavy-handed." The other investigator said Subject told [redacted] and [redacted] disobeyed [redacted] order to not hold the briefing because it contained classified or sensitive information; however, the FBI PowerPoint briefing was reviewed and confirmed to be unclassified. There were two individuals named in the briefing for case study purposes, but there was no record of ITMS investigations for these individuals. A search through the Foreign Influence Task Force of federal law enforcement agencies responsible for conducting investigations involving foreign researchers showed no past or present investigations for these individuals.

The investigators' supervisor, [redacted] InfoSec), [redacted] InfoSec, stated [redacted] OSY, [redacted] told [redacted] "a political" wanted the security clearances for [redacted] and [redacted] suspended because they had an FBI briefing when they were told not to; and that [redacted] instructed [redacted] to suspend their security clearances without supplying many details. [redacted] InfoSec said [redacted] OSY subsequently told [redacted] to re-instate the clearances with no explanation. The investigator's supervisor said [redacted] had never been given such little information by [redacted] OSY to suspend clearances.

[redacted] NIST met with Subject following the FBI briefing. [redacted] said Subject was very angry that the FBI briefing had taken place because [redacted] and [redacted] defied Subject's order. [redacted] NIST felt Subject's anger was an overreaction and that Subject "had it in" for [redacted] and [redacted]. [redacted] thought Subject was "calling the shots," not [redacted] OSY.

[redacted] OSY's then-supervisor was interviewed and said [redacted] had no influence over the suspension or reinstatement of the security clearances. [redacted] said [redacted] directed [redacted] OSY to have OSY provide briefings to NIST, but [redacted] failed to do so. [redacted] described Subject as a "stickler on rules," and that [redacted] got upset when people did not abide by them. [redacted] said [redacted] OSY was angry [redacted] and [redacted] disobeyed [redacted] order not to hold the FBI briefing and said, "We can take their clearances."

One NIST employee who was involved in this matter believed "someone" felt personally insulted because NIST went through with the FBI briefing and that person overreacted

by suspending the clearances. [redacted] opined suspending the clearances was an emotional reaction. Another NIST employee said [redacted] OSY appeared very angry that the FBI briefing took place because [redacted] told NIST to stand down. [redacted] said Subject treated everyone like they were guilty, acted as "judge, jury, and executioner," and stalled security clearance investigations. This NIST employee opined Subject placed an enormous amount of internal negative pressure on [redacted] OSY in an internal battle for control.

[redacted] OSY said that sometime in the [redacted], [redacted] told [redacted] NIST not to move forward on the FBI briefing and that OSY would provide it because ITMS could offer more catered briefings to NIST leadership than the FBI. [redacted] OSY thought Subject had communications with [redacted] and [redacted] telling them not to hold the FBI briefing. [redacted] OSY claimed the InfoSec investigation affirmed candor issues because [redacted] and [redacted] blamed each other for scheduling the briefing and showed disregard for OSY's order not to hold the briefing. A review of the interviews conducted by InfoSec showed [redacted] and [redacted] did not blame each other for facilitating the FBI briefing. They both said [redacted] facilitated the briefing.

[redacted] OSY said InfoSec recommended suspension of the security clearances following their InfoSec investigation, and [redacted] concurred. [redacted] said NIST petitioned to have the clearances reinstated. [redacted] OSY stated Subject did not have influence over the security suspensions and it was not retaliatory. However, a review of Subject's e-mails showed [redacted] OSY forwarded an e-mail from NIST to Subject where NIST requested [redacted]'s clearance to be reinstated and [redacted] OSY asked Subject [redacted] thoughts on it.

Subject denied having a say in the security clearances being suspended. Subject knew [redacted] and [redacted] planned an unclassified briefing by the FBI and that [redacted] OSY told them not to, but they proceeded with the briefing. Subject said a meeting was held in a sensitive compartmented information facility (SCIF) with [redacted] [redacted] OSY, and [redacted] NIST, but Subject could not recall if they told [redacted] NIST to not hold the FBI briefing. Subject said [redacted] and [redacted] OSY were concerned the briefing could alert people at NIST who were engaged in conduct cited in the briefing. However, Subject requested a list of briefing attendees after the briefing was given and does not appear to have knowledge of attendees prior to the briefing.

Subject discussed a meeting [redacted] had with [redacted] and [redacted]; [redacted] OSY; and possibly [redacted], [redacted] OSY, wherein [redacted] and [redacted] were told to stand down on the FBI briefing. Subject did not recall if [redacted] saw the FBI

PowerPoint briefing and did not recall specific interactions [redacted] had with NIST regarding the briefing. A review of e-mails showed Subject did have correspondence with NIST citing Department Security Manual Chapter 36 policy and DOO 20-6 as leverage to say NIST could not hold the briefing.[2] The e-mail review also showed Subject designated an ITMS special agent as the point of contact for the FBI briefing—not NIST. [redacted] stated that prior to the FBI briefing [redacted] provided a copy of the FBI briefing to Subject during a meeting in a SCIF and that Subject reviewed the briefing and pointed out something in it to [redacted] OSY. A review of e-mails also showed [redacted] offered for Subject to obtain a copy of the briefing from [redacted]. Subject did not recall having a conversation with [redacted] OSY to discuss suspending the security clearances. Subject did not know why the clearances were reinstated.

The investigation indicates OSY had almost a year to provide a briefing to NIST from NIST's initial request and failed to do so, even after being directed by [redacted] OSY's supervisor. The briefing was supported through NIST leadership out of concerns for foreign talent recruitment in their laboratories. Instead of providing the briefing, Subject and [redacted] OSY told NIST to stand down on the briefing without justification. When [redacted] and [redacted] proceeded with the briefing, their security clearances were suspended. NIST [redacted] supported the briefing because Subject and [redacted] OSY provided no rational explanation as to why the briefing could not be held and failed to provide an alternate briefing for a year. [redacted], NIST, felt it was an important topic to brief to laboratory leadership to mitigate possible issues with foreign influence over foreign researchers. NIST [redacted] impression was that Subject and [redacted] OSY were attempting to improperly control the briefing.

Subject stated during the OIG interview [redacted] could not remember if [redacted] directed NIST not to hold the FBI briefing. However, OIG interviews with others involved and a review of related e-mails showed Subject directed NIST not to hold the FBI briefing. Subject said [redacted] sent e-mails to NIST citing policy [redacted] claimed supported NIST standing down on the briefings; participated in meetings where NIST was told not to hold the meetings; and witnesses believed Subject acted in an angry, retaliatory manner and influenced [redacted] OSY's decision to direct the security clearance suspensions.

[2] Commerce, Office of Privacy and Open Government. *Department Organization Orders 20-6* [online]. https://osec.doc.gov/opog/dmp/doos/doo20_6.html (accessed December 30, 2020).

6. *Allegation: Subject Misused Government Resources by Directing ITMS Personnel to Transport [redacted] for Personal Travel in a Government Vehicle*

Several witnesses related Subject attended classes at [redacted] on personal time, but that [redacted] had ITMS personnel drive [redacted] to the airport in a government vehicle and that [redacted] flew armed without a flying armed policy in effect. A review of Subject's personnel and training file and information received from [redacted] Department's Project and Administrative Management Division, revealed Subject attended one [redacted] course at [redacted] in [redacted] that was paid for by the Department. However, Subject was interviewed and affirmed [redacted] also attended classes at [redacted] sometime between [redacted] for [redacted] degree program and that these classes were not paid for with Department funds. Subject said [redacted] flew to [redacted] three to four times for [redacted] degree program, which was not funded by the Department and that [redacted] ITMS, gave [redacted] rides to the airport in a government vehicle. [redacted] was interviewed and affirmed [redacted] gave Subject rides to the airport several times in a government vehicle. [redacted] was under the impression the trips were work related. [redacted] did not recall if Subject flew armed.

The evidence establishes that Subject fell short of [redacted] duty to protect and conserve government property and further allowed for its use for unauthorized purposes, as prohibited by 5 C.F.R. § 2635.704. Moreover, based on Subject's acknowledgement that [redacted] travel to the airport was in furtherance of personal travel, significant evidence exists supporting a finding that Subject's misuse of the government vehicle was willful, as enumerated in 31 U.S.C. § 1349. OIG is providing this evidence of the latter violation to agency management for its determination of a § 1349 violation.

Subject also violated 5 C.F.R. § 2635.705(b), Use of a Subordinate's Time by having [redacted] transport [redacted] to the airport in a government vehicle during work hours, for non-work related travel.

7. *Allegation: Subject Improperly Obtained a Unique Flying Armed Number (UFAN) and ITMS Has Operated without a Flying Armed Policy Since [redacted]*

Transportation Security Administration (TSA), Law Enforcement Liaison Section related OSY applied for and was approved for a UFAN, which authorized Subject to fly armed possibly as early as [redacted]. A UFAN is a number unique to each federal law enforcement agency which is required to be given to be verified by TSA every time a federal law enforcement officer flies armed. The request from OSY was encrypted and unable to be accessed. TSA confirmed Subject was the primary point of contact for the

UFAN, and that on [redacted] Subject e-mailed TSA asking for an updated UFAN. TSA affirmed a valid flying armed policy would have been required as part of the approval process for a UFAN. During an interview with Subject, [redacted] affirmed ITMS never had an approved flying armed policy. Subject could not recall if [redacted] was the person who applied for the initial UFAN and what was submitted for a flying armed policy. Interviews of ITMS personnel and management determined there had never been an approved flying armed policy authorizing ITMS agents to fly with their assigned firearm. Based on the absence of an approved flying armed policy for ITMS, Subject either provided or authorized in [redacted] position as [redacted] an unofficial flying armed policy to be used to obtain a UFAN. Subject allowed ITMS agents to fly armed since [redacted] without an official flying armed policy in place.

8. *Allegation: Subject Created a Toxic Work Environment*

Several former ITMS SAs complained they were targeted by Subject for questioning policy, authority, and practices. Interviewees related Subject "stove-piped" everything, discouraged "thinking out of the box" and proactive initiatives and instituted discipline for simply making contacts outside ITMS without [redacted] approval. Several individuals interviewed expressed concern about retaliation from Subject for providing information for this investigation based upon their past experiences with Subject.

The following individuals told OIG during interviews the Subject disciplined them or fired them for questioning [redacted] management and rules:

[redacted] (Complainant)—Complainant filed a [redacted] complaint against Subject, which was substantiated. According to interviews and document reviews, while Complainant was on [redacted], Subject searched [redacted] office for case notes. During the office search, Subject found a classified disc, and reported it to security; but it was deemed not to be a security violation. Subject then searched Complainant's e-mail for the case notes, discovered evidence of an all-day meeting [redacted] believed Complainant attended, compared the date of the meeting to WebTA, and noted Complainant did not take leave for the meeting. When Complainant returned from [redacted] Subject confiscated [redacted] badge and gun and put [redacted] on administrative tasks.

Complainant attested [redacted] uploaded [redacted] notes to CNET prior to going [redacted] and Subject could have accessed them there. Complainant stated the all-day meeting was with the [redacted] and was for information sharing on similar

cases. Complainant said Subject had directed ITMS agents to reach out to this agency for assistance with these particular cases.

Subject was interviewed and cited the following issues with Complainant:

1. Complainant had "an angry outburst" over something another complainant wanted [redacted] to do regarding a case review.
2. Discrepancies between what Complainant put in [redacted] daily activity report and what was noted in CNET.
3. Complainant, prior to [redacted], drafted an affidavit for a search warrant and was setting up a meeting with the Assistant U.S. Attorney (AUSA), without supervisory review. Subject felt misled because Complainant indicated the meeting with the AUSA had not happened, but Subject believed it had already happened.
4. Complainant attended the meeting at [redacted], without informing Subject (same meeting above noted).
5. Complainant, prior to [redacted], did not provide Subject with FBI correspondence regarding a case, as Subject requested.
6. Complainant allegedly left a classified disc in plain view, while on [redacted] which Subject found during the above noted search. Subject reported it to Security, and Security determined no security violation occurred.

Subject consulted with Office of Human Resources (OHR) and OGC to pull e-mails and suspended SA's law enforcement duties based on the above issues.

OHR and OGC confirmed they were involved with the issues related to Complainant. OHR said removal was going to be proposed, but Complainant quit. A [redacted] investigation conducted by the [redacted] determined Subject discriminated against Complainant for taking the above actions [redacted].

E-mail reviews and interviews gave no evidence that Subject discussed any of these issues with Complainant and that Complainant e-mailed numerous concerns to Subject which went unanswered. This included Complainant requesting a reason for the suspension of [redacted] law enforcement authority, revocation of access, and objections to performance rating input. E-mail reviews also showed Complainant made numerous requests for meetings with Subject and Subject was unresponsive. E-mail reviews also revealed Subject obtained Complainant's time and attendance while Complainant was assigned to a different supervisor, obtained badging records, and asked how [redacted] could

obtain e-mails for Complainant's [redacted] account without [redacted] knowing.

[redacted] SA 5)—SA 5 questioned USMS deputation authority and Subject's guidance on "putting everything" on their classified case management system, CNET, so that the information would be less discoverable. SA 5 said Subject told [redacted] did not think SA 5 could ever be promoted because [redacted] was a [redacted], was not a protected class, and could be [redacted]. SA 5 said if Subject did not like you, [redacted] would "target" you. SA 5 felt uneasy on a daily basis that Subject would target [redacted] and try to fire [redacted] for lying on official documents, then take [redacted] clearance, and fire [redacted] for questioning authorities and ITMS policies and procedures. Subject related SA 5 had performance issues and might have said something untrue, but [redacted] could not say what because another former supervisor dealt with them. SA 5 quit ITMS prior to any action being taken against [redacted]

[redacted] SA 3)—SA 3 said Subject operated with a "controlling attitude." SA 3 explained Subject required daily morning phone calls to keep tabs and would not allow anyone to send out e-mails or make contacts to include other law enforcement agents or prosecutors without [redacted] approval.

Interviews and document reviews revealed Subject initiated an investigation into SA 3 after [redacted] received information from "another agency" and learned SA 3 queried [redacted] in a law enforcement database. ITMS submitted the issues to OIG, which referred the issue to OSY. A former ITMS agent who was interviewed noted when OIG declined to investigate, Subject stated, "We can't let [redacted] get away with this" and opened an investigation without knowledge of [redacted] leadership. As part of the ITMS investigation, Subject directed a trash pull on SA 3's house. A picture of an ITMS supervisor with a riflescope drawn over [redacted] head was found during the trash pull. Subject directed a search warrant affidavit be drafted for SA 3's house based on the photo found in the trash pull and e-mails to the ITMS supervisor which 'seemed threatening.' SA 3 was put on telework for [redacted], then administrative leave for almost [redacted] during this investigation. [redacted] then went on [redacted] for [redacted], and quit. SA 3 filed a complaint to the [redacted] relative to this situation and received a settlement. Subject was not directed to conduct this investigation by [redacted] superiors. Without direction by [redacted] leadership, Subject took it upon [redacted] to conduct this extensive and overarching investigation of [redacted] subordinate.

[redacted] (SA 6)—SA 6 described ITMS as a "toxic" environment. [redacted] said Subject was the "most incompetent person" [redacted] ever came across and that Subject had no knowledge of how to conduct an investigation. SA 6 gave Subject notice [redacted] was

quitting and scheduled a meeting with [redacted] OSY, Subject's [redacted] to discuss Subject's mishandling of a work incident. The meeting was placed on a public calendar by [redacted] Hours before SA 6's meeting with [redacted] Subject—accompanied by OHR—told SA 6 [redacted] was [redacted] and had the option to quit or be fired for time and attendance issues.

In an interview with Subject, [redacted] claimed there were time and attendance issues, specifically that SA 6 was not conducting the work [redacted] claimed based on a comparison of notes and work produced. Subject could not recall if [redacted] ever discussed this concern with SA 6 prior to forcing [redacted] termination. Subject claimed [redacted] did not know SA 6 had a meeting scheduled with [redacted]

SA 6 insisted [redacted] was never counseled and never received a negative performance evaluation from Subject. SA 6 believes [redacted] was forced to resign for scheduling the meeting with [redacted] and for questioning Subject about deputation authority, ITMS policies and procedures, and mismanagement of cases. SA 6 thought Subject found [redacted] inquiries "personally insulting."

SA 6 felt pressured by Subject to resign on [redacted] because [redacted] feared [redacted] would be terminated by Subject to prevent [redacted] from divulging Subject's gross mismanagement to [redacted]

[redacted] SA 7)—SA 7 said [redacted] questioned Subject about cases they were investigating because they lacked merit and questioned Subject's statements that case notes were not discoverable. SA 7 felt Subject punished [redacted] for the inquiries by keeping [redacted] off administrative searches. SA 7 stated Subject wanted [redacted] to write an affidavit for a search warrant and SA 7 said there was no probable cause. Subject got irritated, told [redacted] to write it up anyway, and they would find the probable cause. SA 7 said Subject gets angry if anyone contacts an individual outside of ITMS without [redacted] permission.

Interviews, document reviews, and e-mail reviews provided Subject conducted a case review with SA 7 and felt there was a discrepancy between [redacted] daily reports and what was in CNET. Subject searched SA 7's office for additional notes then removed SA 7 from case work while Subject reviewed all [redacted] cases. The following day, SA 7 gave Subject notice [redacted] was [redacted]. During SA 7's final [redacted], Subject had [redacted] work on a policy that SA 7 had already re-written and required [redacted] to provide the link for every search [redacted] conducted while updating the policy. Subject denied SA 7's leave after [redacted] submitted [redacted] notice pending [redacted] productivity on re-writing the policy. Subject attempted to obtain SA 7's badging records, sign in/out logs, CCTV footage, e-mail, Weblogs, and phone records. SA 7 affirmed, prior to this instance, [redacted]

was never counseled for anything. [redacted] described Subject as "vindictive" and "incompetent."

Subject appears to have disciplined SA 7 for questioning [redacted] mismanagement and rules.

[redacted] SA 8)—SA 8 said whenever [redacted] had questions about policies, procedures, or concerns, Subject was 'never available' and 'would always put [redacted] off.' SA 8 said Subject also delayed [redacted] attendance to Criminal Investigation Training Program (CITP) at Federal Law Enforcement Training Center (FLETC) for the [redacted] SA 8 was employed with ITMS. SA 8 suspected Subject might have had an issue with [redacted] because Subject wanted [redacted] to attend CITP the first couple of weeks of [redacted] employment, but SA 8 had scheduled [redacted] and could not attend. Every time thereafter SA 8 asked to go to CITP, Subject 'brushed [redacted] off.' SA 8 said the business day before [redacted] was over, Subject presented [redacted] with a one page memo justifying [redacted] termination, but would not let [redacted] retain a copy. SA 8 related the reasons for termination included SA 8 providing a briefing to the Special Security Officer without notifying Subject and having an SCI document in a space rated for only top-secret. SA 8 provided [redacted] had already done re-training for the SCI incident and it did not affect [redacted] clearance renewal. SA 8 noted [redacted] received a good end-of-year evaluation and was never counseled about anything. SA 8 was completely shocked by the termination.

Subject was interviewed and said SA 8 had discrepancies between [redacted] daily reports and CNET. Subject said [redacted] let SA 8 go because [redacted] was [redacted].

E-mail reviews showed SA 8 sent Subject daily work reports the last 2 months of his employment; however, there is no evidence Subject discussed any work productivity concerns with SA 8 during that time.

9. *Allegation: Subject Did Not Follow Security Manager Protocol*

Witnesses related that the Department had a policy that transfers of classified documents from one person to another had to be documented in Security Manager—a Department database. SA 4 said that Subject directed [redacted] not to transfer classified documents to [redacted] in Security Manager. SA 4 said Subject took physical possession of the documents, but would list them in Security Manager as belonging to SA 4. SA 4 found those documents, some of which were SCI, placed by Subject in the wrong case files.

Chapter 22.4, *Accountability of NSI*, of the Department's *Manual of Security Policies and Procedures*, requires that most classified material, including all top secret information,

"must be properly controlled and accounted for by use of the OSY Security Manager database."[3]

An audit of Security Manager showed that between [redacted], only nine documents, all classified secret, were ever transferred to Subject.

All Subject recalled was [redacted] might have told employees leaving ITMS not to transfer documents to [redacted] in Security Manager because they were still responsible for them.

OIG found evidence of Subject's failure to properly control and account for classified material as required by Chapter 22.4.

10. Allegation: Inappropriate Basis for USMS Deputation for ITMS

Multiple witnesses voiced concerns to Subject that they felt their deputation did not cover them to conduct investigations, and they were limited to conducting protective details. Witnesses related Subject would get angry whenever questioned about the scope of the deputation. In an interview with Subject, [redacted] noted the deputation cited coverage for protection of the Secretary of Commerce and "critical assets." [redacted] initially said the "critical asset" verbiage covered them to conduct investigations, but later admitted [redacted] was unsure exactly what "critical assets" meant. Subject and OGC worked together to obtain the deputation. Subject affirmed carrying a firearm was dependent on the deputation.

In October 2020, the USMS related to OIG and ITMS that ITMS deputation did not extend to conducting investigations and that "critical assets" referred to the protection of facilities in connection with the Secretary of Commerce.

In 2017, OIG looked into a complaint regarding the issue of ITMS deputation after receiving a referral from the USMS citing concerns about ITMS conducting investigations under the deputation. As a result, OIG coordinated with [redacted] who agreed to OIG recommendations to address ITMS scope of authority to conduct investigations under the deputation and to correct deputation for ITMS citing assignment to protection detail. However, subsequent vetting of the deputation resulted in no change to the deputations potentially leaving ITMS agents and the Department in a position of liability for carrying

[3] DOC, 2012. Manual of Security Policies and Procedures. Washington, DC: DOC. Note Subject's activity commenced in [redacted], prior to this version of policy. A prior policy was unable to be obtained.

out duties they were not authorized to do since the inception of the deputation program circa 2011.

11. Allegation: ITMS Failed to Afford the Appropriate Rights, Warnings, or Expectations of Privacy to Interviewees and Searches of Department Employees

Several ITMS agents expressed concern that Garrity and Kalkines rights were not provided to Department employees. In an interview with Subject, [redacted] affirmed ITMS does not have or use Garrity or Kalkines advisement forms, but said they use a non-set verbiage that is akin to Garrity or Kalkines at the beginning of their interviews. Failures to provide appropriate warnings could invalidate statements obtained during the interviews, violate constitutional protections of the interviewees, cause harm to the investigation, and possible liability to the Department.

In [redacted] interview Subject discussed a compilation of what [redacted] believed to be text messages taken from the personal phone of another employee of [redacted] with [redacted] consent. In the exchanges, the individuals discuss their backpacks, purses, and coats being searched by Subject and ITMS. Subject said OGC was consulted about what items could be searched and it was determined that (B)(5) Withholding at Department Request [redacted]. Subject believed some personal items were searched under consent and some without consent because there was no reasonable expectation of privacy due to the items being in a SCIF. OIG interviewed the three OGC attorneys Subject would have contacted for advisement on this matter and none of them recalled talking to Subject about this investigation. This appears to contradict Subject's assertion [redacted] sought advice from OGC. Any concerns about the legality of such searches could have been alleviated if OGC was contacted prior to the searches.

12. Allegation: Subject Routinely Pulled Employees' E-mail to See if they Violated NDAs

A witness related that between [redacted] Subject organized a classified briefing at National Oceanic and Atmospheric Administration (NOAA) in Suitland, Maryland, for individuals associated with satellites, to include the [redacted]. After the briefing, Subject allegedly told witness the real purpose of the briefing was to pull the attendees' e-mails to see if they divulged information covered under the NDAs Subject had them sign in the briefing. The witness felt it was like entrapment. Witness said when [redacted] questioned Subject about the validity of [redacted] intentions, Subject became agitated. Witness did not know if Subject pulled the e-mails or if anyone was disciplined as a result. Due to limited details of the event and limited records regarding ITMS e-mail pulls, OIG was unable to verify if Subject pulled e-mails for the participants of this briefing.

13. Allegation: Subject Directed Inappropriate Searches of Department Employees' Office Spaces

Complainant alleged Subject directed administrative searches to circumvent the need for probable cause and search warrants and directed unlawful "mixed searches," a combination of an administrative and criminal search. Complainant said Subject instructed almost every search to be conducted as an administrative search, even if there was already knowledge of a possible criminal element, and that [redacted] would use the administrative search to get probable cause for a search warrant. Complainant cited an investigation referred to as "The [redacted] Case," wherein a search warrant was executed on an employee's office and then Subject directed an administrative search for areas not covered under the search warrant. The *FLETC Legal Training Handbook* (at 471) states:

> The courts have adopted fairly generous interpretations of *O'Connor* [*v. Ortega*, 480 U.S. 709 (1987)] when confronted with mixed-motive searches. Even assuming that the dominant purpose of the warrantless search is to acquire evidence of criminal activity, the search remains within the *O'Connor* exception to the probable cause and warrant requirement. The government does not lose the capacity and interests of an employer—its special need for the efficient and proper operation of the workplace—merely because the evidence obtained is also evidence of a crime.[4]

Complainant described a warrantless office search conducted by ITMS on [redacted], wherein locked government containers were accessed and a lock picking device was used. Complainant believed the employee had a reasonable expectation of privacy in the locked compartments and said locked compartments are commonly breached by ITMS during administrative searches. Interviews of ITMS agents present for the search revealed locked government compartments were accessed and a lock picking device was used; however, no personal items were searched.

OGC affirmed they provided guidance to ITMS before they conducted warrantless/ administrative searches of Department employee's offices and opined (B)(5) Withholding at Department Request [redacted]. OGC did not recall discussions about using lock picking devices to access locked government compartments, "(B)(5) Withholding at Department Request [redacted].

[4] U.S. Department of Homeland Security. Federal Law Enforcement Training Centers Office of Chief Counsel, *Legal Training Handbook* (2019) [online]. www.fletc.gov/sites/default/files/legal_training_handbook_2019_final.pdf (accessed December 1, 2020).

14. Allegation: Subject Directed Alteration of Documents

Complainant alleged Subject directed another special agent (SA 11) to alter a written statement and the narrative of a subpoena to fit Subject's interpretation of events regarding "The [redacted] Case." Complainant said Subject then directed SA 11 to swear to and sign a search warrant affidavit after Subject made substantive alterations. SA 11 was interviewed and clarified the issue was related to an affidavit for a search warrant on an e-mail account. SA 11 related [redacted] worked with an AUSA in [redacted], but Subject insisted [redacted] review the affidavit and added about five e-mail accounts to be searched. The AUSA [redacted] with the additional e-mails to be searched because (b) (5) [redacted]. The affidavit went back and forth between Subject and the AUSA several times and the AUSA became irritated. SA 11 swore out the AUSA-approved affidavit without Subject's final approval. Subject was annoyed and felt SA 11 colluded with the AUSA. SA 11 believed Subject was going to counsel SA 11 for insubordination, but another agent discouraged disciplinary action. While Subject's actions appeared inappropriate, there was no evidence to support that [redacted] added false information into the affidavit.

15. Allegation: Subject Committed Travel Fraud to [redacted] Virginia

ITMS special agents related they believed Subject might have committed travel fraud during a trip to [redacted] Virginia, from [redacted] for [redacted] Training. The special agents related Subject left the training for 1 night after Subject stated [redacted] had to return to the office. Global positioning service information left on from an earlier surveillance training exercise showed Subject did not go to the office, but stayed at [redacted] residence for the night. A review of Subject's travel voucher showed [redacted] claimed lodging for every night from [redacted] however, there was a justification that [redacted] needed to return to [redacted] residence due to lack of internet connectivity and the place of lodging would not allow [redacted] to check out for 1 night and check back in. Subject also claimed a reduced per diem rate for the 2 partial days at home.

COORDINATION WITH U.S. DEPARTMENT OF JUSTICE

On February 4, 2020, the U.S. Public Integrity Office (PIN), Department of Justice, Washington, DC, did not assume this case for prosecution. Following additional investigation, on September 8, 2020, OIG presented details developed after coordination with PIN to the U.S. Attorney's Office, Washington, DC (USAO DC), and USAO DC declined to pursue prosecution. This investigation is being provided to the Office of the Secretary for review and consideration of appropriate action.

INDEX OF PERTINENT CASE FILE DOCUMENTS

CMS Document No.	Description
1	DOC-OIG-19-06-20-0002 (Initial Compl.) (June 21, 2019)
3	Additional Information (June 21, 2019)
6	IRF—Basis for Investigation (July 25, 2019)
7	IRF—Interview of [redacted] (July 26, 2019)
8	IRF—Interview of [redacted] (July 26, 2019)
9	IRF—Interview of [redacted] (July 24, 2019)
10	IRF—Interview of [redacted] (July 29, 2019)
11	IRF—Interview of [redacted] (Aug. 5, 2019)
12	IRF—Interview of [redacted] (Aug. 5, 2019)
13	IRF—Interview of [redacted] (Aug. 5, 2019)
14	IRF—Interview of [redacted] (Aug. 6, 2019)
15	IRF—Interview of [redacted] (Aug. 6, 2019)
18	IRF—Request for E-mails (Aug. 30, 2019)
20	IRF—Interview of [redacted] (Sept. 6, 2019)
21	IRF—Receipt of NDAs (Sept. 18, 2019)
22	IRF—Interview of [redacted] (Oct. 1, 2019)
23	IRF—Interview of [redacted] (Sept. 30, 2019)
24	IRF—Interview of [redacted] (Oct. 17, 2019)
25	IRF—Interview of [redacted] (Oct. 21, 2019)
26	IRF—OS ITMD Officials E-mail Review 10.29.19 (Oct. 17, 2019)
27	IRF—Interview of [redacted] (Feb. 11, 2020)
28	IRF—Review of Travel for [redacted] (Feb. 13, 2020)
29	IRF—Receipt of UFAN Information (Sept. 14, 2019)
30	IRF—Interview of [redacted] (Feb. 19, 2020)
31	IRF—Information Received from [redacted] (Feb. 24, 2020)
32	IRF—Interview of [redacted] (Feb. 25, 2020)
33	IRF—Information Received from [redacted] (Mar. 23, 2020)
34	IRF—Interview of [redacted] 8-21-2020 (Aug. 24, 2020)
35	IRF—Consultation with Prosecutor (Aug. 26, 2020)
36	IRF—Interview of [redacted] (Aug. 24, 2020)
37	IRF—Interview of [redacted] (Aug. 27, 2020)
38	IRF—Interview with [redacted] (Aug. 26, 2020)

CMS Document No.	Description
39	IRF—Interview of [redacted] (Aug. 27, 2020)
40	IRF—Consultation with OGC Regarding CM Recordings (Aug. 25, 2020)
41	IRF—Interview of [redacted] (Aug. 27, 2020)
42	IRF—Interview of [redacted] (Aug. 31, 2020)
43	IRF—Information Regarding [redacted] and [redacted] (Aug. 29, 2020)
44	IRF—Interview of [redacted] (Sept. 3, 2020)
45	IRF—Interview of [redacted] (Sept. 3, 2020)
46	IRF—Interview of [redacted] (Sept. 3, 2020)
47	IRF—Interview of [redacted] (Sept. 4, 2020)
48	IRF—Interview of [redacted] (Sept. 5, 2020)
49	IRF—Interview of [redacted] (Sept. 8, 2020)
50	IRF—Interview of [redacted] (Sept. 4, 2020)
51	IRF— [redacted] Complain from 20-1028 (n.d.)
52	IRF—E-mail update from DOC OIG to [redacted] (Sept. 10, 2020)
53	IRF—Interview of [redacted] 9-3-2020 (Sept. 10, 2020)
54	IRF—Consultation with Prosecutor—D.C.—9-4-2020 (Sept. 11, 2020)
55	IRF—Interview of [redacted]—9-10-2020 (Sept. 11, 2020)
56	IRF—Interview of [redacted] (Sept. 14, 2020)
57	IRF—Request for CNET Access—NS3 (DOC) (Sept. 14, 2020)
58	IRF—Review of Travel for [redacted] (Feb. 13, 2020)
59	IRF—Interview of [redacted] (Sept. 15, 2020)
60	IRF—Interview of [redacted] (Sept. 16, 2020)
61	IRF—Interview of [redacted] (Sept. 17, 2020)
62	IRF—Badging Information Received for [redacted] (Sept. 17, 2020)
63	IRF—Interview of [redacted] (Sept. 19, 2020)
64	IRF—Interview of [redacted]—9-15-2020 (Sept. 19, 2020)
65	IRF—Interview of [redacted] (Sept. 19, 2020)
66	IRF—Consultation with OC Regarding Unit Head for ITMS (Sept. 22, 2020)
67	IRF—Interview of [redacted] (Sept. 22, 2020)
68	IRF—Interview of [redacted] (Sept. 22, 2020)
69	IRF—Information Received from [redacted] (Sept. 25, 2020)
70	IRF—Interview of [redacted] (Oct. 7, 2020)
73	IRF—Review of USMS E-mail Regarding Special Deputation (Oct. 21, 2020)

CMS Document No.	Description
74	IRF—Information Received from NIST OCIO—[redacted] (Oct. 26, 2020)
75	IRF—Information Received from OS OCIO—[redacted] (Oct. 26, 2020)
76	IRF—Information Received from FIWG (Oct. 26, 2020)
77	Garrity Interview—[redacted] E-mail (Oct. 23, 2020)
78	IRF—Information Received from [redacted] (Oct. 26, 2020)
79	IRF—Information from [redacted]—ITMS Job Descriptions—[redacted] Programs (Oct. 27, 2020)
80	IRF—Consultation with USMS Regarding ITMS Deputation (Oct. 27, 2020)
81	IRF—Review of [redacted] USMS Special Deputation Documents (Oct. 27, 2020)
82	IRF—Information Received Regarding [redacted] Badge and Credentials (Oct. 29, 2020)
83	IRF—Document Review of DOC/OSY Case File 20090417 (Oct. 30, 2020)
84	IRF—Information Regarding FMLA for [redacted] (Oct. 29, 2020)
85	IRF—Interview of [redacted] (Nov. 6, 2020)
86	IRF—Interview of [redacted] 11-6-2020 (Nov. 6, 2020)
87	IRF—Search of [redacted] Office (Nov. 4, 2020)
88	IRF—Interview of [redacted] (Nov. 7, 2020)
89	IRF—Interview of [redacted] (Nov. 5, 2020)
90	IRF—Records Review on CNET (Nov. 9, 2020)
91	IRF—Coordination with TSA Regarding OSY UFAN (Nov. 12, 2020)
92	IRF—Interview of [redacted] (Nov. 13, 2020)
93	IRF—Review of Documents Collected from [redacted] Office (Nov. 13, 2020)
94	IRF—Interview of [redacted]—11-13-2020 (Nov. 13, 2020)
95	IRF—Interview of [redacted] (Nov. 16, 2020)
96	IRF—Interview of [redacted] (Nov. 20, 2020)
97	Closure Memo—17-0976 (Aug. 2, 2017)
98	IRF—Email Review (Oct. 30, 2020)
99	IRF—Interview of [redacted] Follow-up Questions (Dec. 14, 2020)
100	IRF—Interview of OGC Regarding Searches of [redacted] Employees Belongings (Dec. 16, 2020)
101	IRF—Information Regarding [redacted]—OIG Email Request by [redacted] (Dec. 18, 2020)
102	IRF—WebTA Information Received for [redacted] (Dec. 18, 2020)
103	IRF—Interview of [redacted] (Dec. 18, 2020)

CMS Document No.	Description
104	IRF—Information Received from [redacted] (Dec. 18, 2020)
105	IRF—Information Received from BIS OCIO (Nov. 2, 2020)
106	IRF—Review of Media Collected from [redacted] Office by [redacted] (Dec. 23, 2020)
107	IRF—Information from Subject's Former Supervisors Regarding Travel to [redacted] (Feb. 16, 2021)