All Withholdings (B)(6) & (B)(7)(C)

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

MEMORANDUM FOR: [redacted]
Tactical Operations Division
United States Marshals Service (USMS)

FROM: [redacted]
Office of Criminal Investigations [redacted]

DATE: August 2, 2017

SUBJECT: Referral from USMS to Department of Commerce Office of Inspector General

On May 22, 2017, the Department of Commerce (DOC), Office of Inspector General (OIG), Office of Investigations (OI) received the referral from your office dated May 12, 2017. The referral contained an email that raised concerns about the special deputations of, and possible overreaching of authority by, agents assigned to the DOC Office of Security's (OSY) Investigations and Threat Management Division (ITMD).

A preliminary investigation generally unsubstantiated the allegations. The justification for special deputations does not appear to have been falsified, and the international incident described in the email was discredited as a misrepresentation of a benign domestic occurrence. We did, however, find some assignment designation concerns in the USM-3B Forms of ITMD personnel. At the completion of this inquiry, I briefed the DOC [redacted] of our findings and concerns. The [redacted] assured us the verbiage on the USM-3B Forms would be revisited and re-coordinated with USMS if necessary. [redacted] also assured us [redacted] office had recently increased oversight of ITMD investigations and would further research ITMD's authority requirements and limitations.

For any questions or concerns, I can be reached at [redacted] or [redacted].

All Withholdings (B)(6) & (B)(7)(C)

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

MEMORANDUM FOR: The File

FROM: [redacted]
Office of Criminal Investigations

DATE: August 2, 2017

SUBJECT: Action Memorandum for Closure
17-0967: ITMD Deputation (OS/OSY)

On May 22, 2017, the Department of Commerce (DOC), Office of Inspector General (OIG), Office of Investigations (OI) received a referral from the U.S. Marshals Service (USMS). The referral contained an email from a person purporting to be part of the DOC Executive Protection Unit (EPU; aka Protection Detail) and raised concerns about the Special Deputations of, and possible overreaching of authority by, agents assigned to the Office of Security's (OSY) Investigations and Threat Management Division (ITMD). A similar complaint (17-0462-H) was addressed by an H-referral response from the Office of Secretary (OS). However, additional details and allegations in the complaint forwarded by USMS warranted preliminary investigation by DOC OIG.

Allegations and investigative activity:

The complaint contained three allegations summarized as follows:

1. ITMD obtains Special Deputation from USMS to conduct protection for the Secretary of Commerce but uses it to conduct investigations.
2. ITMD sent an agent overseas in an undercover status without following protocol, and perhaps in excess of their authority, resulting in detention of the agent.
3. ITMD's cases target persons primarily of a particular ancestry.

Pursuant to these allegations, DOC OIG took the following investigative steps:

1. Obtained and reviewed all Special Deputation documents USMS had on file for DOC agents (including EPU and ITMD agents).

2. Reviewed documents (DOO, DAO, and duty descriptions) provided by OS pursuant to their response to 17-0462-H.
3. Interviewed the USMS [redacted].
4. Coordinated with the OIG for the Intelligence Community to obtain potential points of contact regarding authority for units conducting counter-intelligence investigations. Determined the counsel for the Office of the Director of National Intelligence could likely assist in authority issues and application of Title 50, Unites States Code.
5. Interviewed the [redacted].

Findings:

Allegation 1: The investigation did not substantiate any falsification of USMS Special Deputation documents. The justification sections and duty descriptions to support deputation were truthful and discretely differentiated ITMD agents from EPU personnel. However, the Form USM-3B (Special Deputation Oath of Office, Authorization and Appointment) for every applicant listed "PROTECTION DETAIL" under the name of the agent, whether EPU or ITMD. An interview of the [redacted] revealed ITMD agents do, on occasion, assist EPU with protection missions. While it is likely necessary to include some mention of protection on the USM-3B since ITMD agents might serve on protection missions, it seems at least equally important that this form shows each ITMD agent as being assigned to an investigative unit. Their primary mission and need for authority conveyed by USMS Special Deputation is investigative in nature. An interview of the USMS [redacted] revealed ITMD could obtain Special Deputations based upon their investigative mission that takes them outside of DOC facilities and the deputations were not contingent on the protection mission. The USMS [redacted] also stated the USM-3B is completed by USMS personnel. Based upon the totality of the facts developed, there was no indication of falsification of deputation documents by ITMD personnel, but the listing of ITMD agents solely as Protection Detail personnel on the USM-3B could be problematic to their investigative mission.

Allegation 2: An interview of the [redacted] revealed there was no such incident in which an ITMD agent was sent overseas and detained in the presence of EPU agents. [redacted] did describe an incident at an event in DC where an ITMD agent conducting surveillance at the event was mistaken for someone from a foreign delegation by International Trade Adminstration and EPU personnel. The agent was approached and revealed [redacted] as an ITMD agent. Thus, this allegation was deemed unsubstantiated.

Allegation 3: The case(s) described in the complaint as targeting persons of a certain ancestry involve the possible recruitment by a certain country's government of U.S.-based persons with ancestry from that country. Thus, the subjects are likely to be of a certain ancestry. OIG has been brought into a few of these cases based upon fraud and other OIG-purview offenses included in the schemes, providing a basis of knowledge of these cases. OIG agents working on these cases have observed no reason to believe racial, ethnic, or cultural bias is a motivator in these cases. This allegation was deemed unsubstantiated.

Coordination:

On July 26, 2017, [redacted] met with [redacted], and briefed [redacted] on the allegations and findings. [redacted] explained the allegations forwarded to OIG by USMS. [redacted] informed [redacted] of the findings for each specific allegation. [redacted] emphasized [redacted] concern that the listing of ITMD agents on Form USM-3B solely as Protection Detail personnel could create a problem for their investigative authority. [redacted] further suggested someone in the Office of the Secretary (OS) or Office of Security (OSY) seek clarification from the Office of the Director of National Intelligence (ODNI) on ITMD's authority and the possible need to affiliate with the Intelligence Community. [redacted] stated [redacted] would look into working with USMS to have the USM-3B forms for ITMD agents adjusted to reflect their assignment to investigative duties. [redacted] also stated [redacted] would talk to the [redacted] and relevant parties regarding ITMD's authority and the possible need to coordinate with ODNI. [redacted] added that ITMD now provides a monthly briefing on all cases and case activity to [redacted] and/or [redacted] of OSY, and [redacted], providing better oversight of ITMD than before.

Approval:

MARK GREENBLATT

Mark L. Greenblatt, AIGI

OFFICE OF INSPECTOR GENERAL
OFFICE OF INVESTIGATIONS

REPORT OF INVESTIGATION

CASE TITLE:	FILE NUMBER:
[redacted]: [redacted] (OSY) INVESTIGATIONS AND THREAT MANAGEMENT DIVISION (ITMD) OFFICE OF SECURITY (OSY) U.S. DEPARTMENT OF COMMERCE (DOC)	16-0996-W **TYPE OF REPORT:** ☐ Interim ☒ Final ☐ Supplemental

BASIS FOR INVESTIGATION

In April 2016, the OIG received a complaint from [redacted] (the complainant) alleging that [redacted], and [redacted] (subjects), of the Investigations and Threat Management Division (ITMD) in the DOC Office of Security (OSY), retaliated against [redacted] due to disclosures of prohibited personnel practices, sexual harassment, security violations, and gross mismanagement that [redacted] made to various DOC officials. The complainant alleged that, in retaliation for these disclosures, [redacted] and [redacted] had (1) refused to deputize [redacted] (2) initiated an investigation on [redacted] (3) removed [redacted] from [redacted] official workplace and placed [redacted] in a full-time telework from home status; (4) suspended [redacted] security clearance; and (5) suspended [redacted] government email account.[1]

METHODOLOGY

The OIG conducted interviews and reviewed pertinent documents. Specifically, the OIG interviewed the complainant; two subjects; [redacted], OSY; [redacted], ITMD; [redacted], Office of Human Resources and Management (OHRM); [redacted], Information and Personnel Security Division, OSY; [redacted], ITMD; and [redacted],

[1] CMS entry No. 1, attach.

Distribution: OIG X Bureau Organization/Agency Management X DOJ: ____ Other (specify):			
Signature of Case Agent: [redacted]	Date:	Signature of Approving Official: MARK GREENBLATT	Date:
Name/Title: [redacted]		Name/Title: Mark Greenblatt / Assistant Inspector General for Investigations	

FOR OFFICIAL USE ONLY

This document remains the property of the Office of Inspector General and is provided to you for official use in accordance with your duties. This document may contain law enforcement sensitive information as well as be protected by the Privacy Act, 5 U.S.C. § 552a. Per DAO 207-10, do not disclose or disseminate this document or the information contained herein, or otherwise incorporate it into any other records system, without prior written permission from the Office of Inspector General. Public release will be determined by the Office of Inspector General under the terms of the Freedom of Information Act, 5 U.S.C. § 552, and the Privacy Act, 5 U.S.C. § 552a. Requests for copies of this report must be referred to the Office of Inspector General in accordance with DAO 207-10.

, OHRM. Further, the OIG reviewed email correspondences and various government records related to the allegations.

RESULTS OF INVESTIGATION

The OIG concluded that the allegation that and retaliated against the complainant for making disclosures about prohibited personnel practices, sexual harassment, security issues, and gross mismanagement to various DOC officials is unsubstantiated. In particular, the OIG found that the complainant has not established that disclosures were contributing factors to the personnel actions taken against Further, the OIG's analysis established that the agency has presented clear and convincing evidence that it would have taken the same personnel actions in the absence of the complainant's disclosures.

DETAILS OF INVESTIGATION

I. Facts

In , the complainant began a position as a within the Department of Commerce's Office of Security (OSY) Investigations and Threat Management Division (ITMD). After starting this position, the complainant learned that had the Basic Agent Test (BAT) that was mandatory for all ITMD agents to complete. had the BAT in an effort to ensure that new agents learned their duties as well as ITMD procedures. included the BAT requirement in the vacancy announcement under which the complainant was hired.

On , sent an email to the complainant and other ITMD agents stated that "ITMD Special Agents are required to successfully complete Basic Agent Training (BAT) per the vacancy announcement (for new agents)."[2] The email noted that "[f]ailing to remediate or additional failures of testable blocks of instruction will result in the agent being processed for administrative action."[3] On , contacted , a in DOC's OHRM, to discuss options for a newly hired employee who was not satisfactorily passing the BAT.[4] On September 13, 2015, OHRM issued guidance to that " can't own program and test an employee and if they don't meet standards try to punish/remove the employee."[5] noted that "[i]f is concerned with the selectee performance, can create a performance

[2] CMS entry No. 19, at 4.
[3] *Id.*
[4] *Id.* at 6.
[5] *Id.*

FOR OFFICIAL USE ONLY

This document remains the property of the Office of Inspector General and is provided to you for official use in accordance with your duties. This document may contain law enforcement sensitive information as well as be protected by the Privacy Act, 5 U.S.C. § 552a. Per DAO 207-10, do not disclose or disseminate this document or the information contained herein, or otherwise incorporate it into any other records system, without prior written permission from the Office of Inspector General. Public release will be determined by the Office of Inspector General under the terms of the Freedom of Information Act, 5 U.S.C. § 552, and the Privacy Act, 5 U.S.C. § 552a. Requests for copies of this report must be referred to the Office of Inspector General in accordance with DAO 207-10.

standard/element."[6] subsequently changed the BAT element from a mandatory requirement to a performance-plan element on the ITMD special agent vacancy announcement, .

On , the complainant contacted and questioned the BAT testing requirement. The complainant stated that did not believe that had the authority to require agents to complete this test as a condition of their continued employment with OSY. On , notified the complainant that the BAT requirement should not have been included in the vacancy announcement, but that may make it an element of the complainant's performance plan.[7]

Following introductory training in Washington, D.C., the complainant moved to permanent duty station in .[8] Before relocating to , the complainant notified that witnessed a ITMD agent make inappropriate sexual comments in front of and about a intelligence officer during their training.[9] Upon receiving this information from the complainant, stated that immediately contacted the intelligence officer about the alleged sexual harassment.[10] In response, told that denied the allegations and stated that it was not harassment. The intelligence officer confirmed that approached about this issue and that denied the allegations.

In , the complainant raised concerns to about the manner in which had directed and another agent to conduct computer searches on background checks.[11] Specifically, had instructed the complainant and colleague to conduct background checks through open source internet search engines on DOC computers. The complainant told that was uncomfortable conducting these searches because they were traceable and could lead to counter-detection. In response, discussed the risks of computer searches with the complainant and met with both agents to train them on how to mitigate risks while conducting the searches. stated that also discussed the risks of conducting computer searches with [12] Though remembered that the security of computer

[6] *Id.*
[7] *Id.* at 9.
[8] CMS entry No. 12 at 1, 4.
[9] *Id.* at 6.
[10] CMS entry No. 21 at 5.
[11] CMS entry No. 23 at 4.
[12] *Id.*

FOR OFFICIAL USE ONLY

This document remains the property of the Office of Inspector General and is provided to you for official use in accordance with your duties. This document may contain law enforcement sensitive information as well as be protected by the Privacy Act, 5 U.S.C. § 552a. Per DAO 207-10, do not disclose or disseminate this document or the information contained herein, or otherwise incorporate it into any other records system, without prior written permission from the Office of Inspector General. Public release will be determined by the Office of Inspector General under the terms of the Freedom of Information Act, 5 U.S.C. § 552, and the Privacy Act, 5 U.S.C. § 552a. Requests for copies of this report must be referred to the Office of Inspector General in accordance with DAO 207-10.

searches was an issue in the office, [redacted] could not recall whether the complainant brought it to [redacted] attention.[13]

The complainant continued to struggle to pass the BAT as the [redacted] progressed. Despite these problems, ITMD submitted the special deputation application for the complainant to the U.S. Marshal's Service (USMS) on [redacted] [redacted].[14] As a supplement to this application, [redacted] also submitted a letter to USMS certifying that [redacted] concurred with the complainant's participation in the Special Deputation Program and that the complainant was not the subject of an internal investigation.[15]

On [redacted], the complainant sent an email to OSY [redacted] stating that [redacted] and [redacted] had mistreated the complainant to the point that it was affecting [redacted] health.[16] On the same day, the complainant went on extended FMLA leave.[17] On [redacted] [redacted], the complainant provided [redacted] with additional information about the alleged mistreatment. The complainant stated that [redacted] was not clearly informed of the BAT requirement when [redacted] applied and interviewed for the ITMD position and that [redacted] had been "unable to adapt to the criminal investigative methods [redacted] [redacted] had in place."[18] The complainant also stated that the BAT testing was "outside of the normal course of [redacted] [redacted] years of conducting criminal investigations" and constituted a prohibited personnel practice, and that [redacted] believed [redacted] had delayed [redacted] deputation because of [redacted] [redacted] the BAT.[19] Further, the complainant stated that [redacted] was wasting government funds by making [redacted] attend training, such as the NEVO driving course, which [redacted] completed years ago. The complainant explained that [redacted] was in fear of losing [redacted] ITMD job.[20]

[redacted] discussed the concerns raised in the complainant's emails with [redacted] in [redacted] [redacted].[21] In addition, [redacted] discussed the complainant's request to transfer to a protection detail with [redacted] and [redacted] OSY [redacted], but there were no openings at that time for this

---

[13] CMS entry No. 21 at 7. On [redacted], the complainant notified an OIG special agent about [redacted] concerns regarding the security of the computer searches. The complainant requested to remain confidential and the OIG did not take further action in this matter until the complainant submitted [redacted] complaint in [redacted]. CMS entry No. 4 at 105.

[14] CMS entry No. 20 at 5.

[15] *Id.* at 7.

[16] CMS entry No. 14 at 3.

[17] CMS entry No. 12 at 8.

[18] CMS entry No. 14 at 45.

[19] *Id.*

[20] *Id.*

[21] CMS entry No. 15 at 4-5.

FOR OFFICIAL USE ONLY

This document remains the property of the Office of Inspector General and is provided to you for official use in accordance with your duties. This document may contain law enforcement sensitive information as well as be protected by the Privacy Act, 5 U.S.C. § 552a. Per DAO 207-10, do not disclose or disseminate this document or the information contained herein, or otherwise incorporate it into any other records system, without prior written permission from the Office of Inspector General. Public release will be determined by the Office of Inspector General under the terms of the Freedom of Information Act, 5 U.S.C. § 552, and the Privacy Act, 5 U.S.C. § 552a. Requests for copies of this report must be referred to the Office of Inspector General in accordance with DAO 207-10.

detail.[22] also discussed the complainant's transfer request with in the DOC Human Resources Office in either or .[23]

On , USMS notified that ITMD's application for the complainant's deputation was approved.[24] responded on , and requested to delay the swearing-in ceremony for the complainant's deputation until returned from . On , USMS informed that a ceremony was scheduled for and asked if the complainant could attend. acknowledged this email on and forwarded it to [25]

The complainant returned from around . In and , became aware of various issues concerning the complainant's conduct. Specifically, learned that the complainant failed to report that went on foreign travel during leave.[26] In addition, the complainant used an unauthorized thumb drive on government computer and failed to protect the combinations of classified spaces and containers.[27] On , the complainant informed that had used LInX, a law enforcement database administered by NCIS that was not authorized for DOC use, to conduct searches, and that access to this database had carried over from previous position at .[28] Following this conversation with the complainant, contacted the LInX program manager at NCIS to report the complainant's unauthorized access. During conversation with the program manager, learned that the complainant had not brought LInX account over from as had claimed; rather, the complainant had gained access to the account through the assistance of one of the complainant's former coworkers, who was also the LInX account manager at [29] spoke with the agent who created the complainant's account, and the agent stated that the complainant told that had permission to access the LInX account. inquired into the searches that the complainant made through LInX account and discovered that the complainant had not run

[22] *Id.* at 4.

[23] *Id.*

[24] CMS entry No. 14 at 39.

[25] *Id.* at 42.The record is unclear as to what happened with the complainant's deputation swearing-in ceremony. The swearing-in was scheduled for the same day that initiated an administrative inquiry into the complainant's misconduct issues.

[26] CMS entry No. 23 at 11..

[27] CMS entry No. 14 at 85.

[28] CMS entry No. 23 at 6, 9; CMS entry No. 14 at 86.

[29] CMS entry No. 23 at 10.

FOR OFFICIAL USE ONLY

This document remains the property of the Office of Inspector General and is provided to you for official use in accordance with your duties. This document may contain law enforcement sensitive information as well as be protected by the Privacy Act, 5 U.S.C. § 552a. Per DAO 207-10, do not disclose or disseminate this document or the information contained herein, or otherwise incorporate it into any other records system, without prior written permission from the Office of Inspector General. Public release will be determined by the Office of Inspector General under the terms of the Freedom of Information Act, 5 U.S.C. § 552, and the Privacy Act, 5 U.S.C. § 552a. Requests for copies of this report must be referred to the Office of Inspector General in accordance with DAO 207-10.

searches of the names that [redacted] had provided to [redacted] instead, the complainant had run a search only of [redacted] own name.[30]

On [redacted], [redacted] issued a memorandum to the complainant notifying [redacted] that OSY was conducting an administrative investigation "based on ongoing concerns regarding your security violations and failure to follow instructions."[31] The memorandum stated that the complainant would be assigned to telework and that [redacted] access to Classified National Security Information was suspended while this investigation was pending.[32] In addition, [redacted] notified the complainant that [redacted] access to [redacted] government email account was also suspended and that [redacted] would therefore need to use [redacted] personal email account to communicate with [redacted] for official purposes while [redacted] was assigned to telework.[33]

On [redacted], the complainant submitted a complaint to the OIG in which [redacted] alleged that [redacted] and [redacted] were committing gross mismanagement in OSY and that they were retaliating against [redacted] In the complaint, the complainant noted that [redacted] had been placed on extended telework pending an investigation into [redacted] request to access the LInX database through a former [redacted] colleague. The complainant alleged that this investigation had limited [redacted] ability to perform [redacted] job duties, was hindering the complainant from returning to [redacted] position at [redacted] and was in retaliation for [redacted] previous complaints to [redacted] and [redacted] In this regard, the complainant stated that [redacted] raised concerns with [redacted] on [redacted], about [redacted] directions for the complainant and another agent to conduct background checks through unsecure Google searches.[34]

On [redacted], [redacted] notified the OIG about OSY's investigation into the complainant's unauthorized use of the LInX database. The OIG determined that it would defer to OSY's investigation into these issues white it continued its investigation into the complainant's retaliation claims.

II. Analysis

The complainant alleged that [redacted] and [redacted] [redacted] retaliated against [redacted] for disclosures [redacted] made to various DOC officials about the BAT requirement, harassment, security issues, and gross mismanagement between [redacted] and [redacted]. Specifically, the complainant alleged that, due to these disclosures, [redacted] and [redacted] (1) refused to deputize

[30] *Id.*

[31] CMS entry No. 1 at 15.

[32] *Id.*; CMS entry No. 23 at 11.

[33] CMS entry No. 23 at 11.

[34] CMS entry No. 1.

FOR OFFICIAL USE ONLY

This document remains the property of the Office of Inspector General and is provided to you for official use in accordance with your duties. This document may contain law enforcement sensitive information as well as be protected by the Privacy Act, 5 U.S.C. § 552a. Per DAO 207-10, do not disclose or disseminate this document or the information contained herein, or otherwise incorporate it into any other records system, without prior written permission from the Office of Inspector General. Public release will be determined by the Office of Inspector General under the terms of the Freedom of Information Act, 5 U.S.C. § 552, and the Privacy Act, 5 U.S.C. § 552a. Requests for copies of this report must be referred to the Office of Inspector General in accordance with DAO 207-10.

[redacted] (2) initiated an investigation on [redacted] (3) removed [redacted] from [redacted] official workplace and placed [redacted] in a full-time telework from home status; (4) suspended [redacted] security clearance; and (5) suspended [redacted] government email account. For the reasons provided below, the OIG found that the complainant has not established that [redacted] and [redacted] actions were in retaliation for the complainant's protected disclosures.

A. Whistleblower Retaliation

1. Legal Standard

The Whistleblower Protection Act (Act) makes it a prohibited personnel practice to take or fail to take (or threaten to take or fail to take) a personnel action with respect to a federal employee or applicant for employment because of any disclosure of information by the employee or applicant that the employee reasonably believes evidences any violation of law, rule or regulation; gross mismanagement; a gross waste of funds; an abuse of authority; or a substantial and specific danger to public health or safety.[35]

In order to establish a *prima facie* case of retaliation, an employee must show that [redacted] made a protected disclosure, and that the disclosure was a contributing factor in a personnel action against [redacted]. The employee may demonstrate that the protected disclosure was a contributing factor in the personnel action through circumstantial evidence, such as evidence that the official taking the action knew of the disclosure and the personnel action occurred within a period of time such that a reasonable person could conclude that the disclosure was a contributing factor in the personnel action.[36] One way for an aggrieved employee or applicant to make this showing is by providing evidence sufficient to meet the "knowledge/timing" test, which requires evidence that (1) the official taking the personnel action knew of the disclosure or protected activity; and (2) the personnel action occurred within a period of time such that a reasonable person could conclude that the disclosure or protected activity was a contributing factor in the personnel action.[37]

The agency can rebut this *prima facie* case if it demonstrates by clear and convincing evidence that it "would have taken the same personnel action in the absence of such disclosure."[38] The key factors in determining whether the agency has met this burden are (1) the strength of the agency's evidence in support of the personnel action; (2) the existence and strength of a

[35] 5 U.S.C. § 2302(b)(8).
[36] 5 U.S.C. § 1221(e)(1).
[37] 5 U.S.C. § 1221(e)(1); *Cassidy v. Department of Justice*. 581 Fed. App'x 846, 851 (Fed. Cir. 2014).
[38] 5 U.S.C. § 1221(e)(2).

FOR OFFICIAL USE ONLY

This document remains the property of the Office of Inspector General and is provided to you for official use in accordance with your duties. This document may contain law enforcement sensitive information as well as be protected by the Privacy Act, 5 U.S.C. § 552a. Per DAO 207-10, do not disclose or disseminate this document or the information contained herein, or otherwise incorporate it into any other records system, without prior written permission from the Office of Inspector General. Public release will be determined by the Office of Inspector General under the terms of the Freedom of Information Act, 5 U.S.C. § 552, and the Privacy Act, 5 U.S.C. § 552a. Requests for copies of this report must be referred to the Office of Inspector General in accordance with DAO 207-10.

retaliatory motive; and (3) the evidence that similarly situated non-whistleblowers were treated similarly.[39]

2. Analysis

The OIG found that, although the complainant has established a *prima facie* case of retaliation, the agency has demonstrated by clear and convincing evidence that it would have taken the same personnel action in the absence of the complainant's disclosures.[40]

The complainant has not established that either [redacted] or [redacted] were aware of the complainant's disclosures to OHRM in [redacted]; however, the complainant's other disclosures between [redacted] and [redacted] appear to satisfy the "knowledge/timing" test. In this regard, [redacted] confirmed that [redacted] recalled the complainant's reports to [redacted] about harassment in [redacted] and the complainant's emails to [redacted] in [redacted] and [redacted]. Although [redacted] did not recall the complainant's disclosures about the security of ITMD's security searches, [redacted] confirmed that the complainant raised these concerns with [redacted] in [redacted] Therefore, [redacted] and [redacted] were both aware of various disclosures that the complainant made in the months prior to the alleged retaliatory actions that occurred in [redacted]. Seven months lapsed between the time the complainant made [redacted] first disclosure to OHRM and [redacted] decision to initiate an internal investigation in [redacted] that resulted in the alleged retaliatory actions. As the evidence indicates that [redacted] and [redacted] were aware of at least some of the disclosures the complainant made in this seven-month period, the complainant has established that the personnel actions occurred within a period of time such that a reasonable person could conclude that the disclosure or protected activity was a contributing factor in the personnel action.[41] As such, the complainant has established a *prima facie* case of retaliation under the provisions of the Act.

---

[39] *Carr v. Social Sec. Admin.*, 185 F.3d 1318, 1323 (Fed. Cir. 1999).

[40] As a threshold matter, the OIG questions whether the complainant's communications with OHRM rose to the level of a protected disclosure. Section 2302(a)(2)(D) of the Act defines a protected disclosure as information that the employee reasonably believes evidences any violation of any law, rule, or regulation; gross mismanagement; a gross waste of funds; an abuse of authority; or a substantial and specific danger to public health or safety. Here, although the evidence indicates that the complainant disagreed with [redacted] decision about the BAT requirement in [redacted] communications with OHRM, it is unclear whether this communication was more than a disagreement over a management decision and rose to the level of a protected disclosure. However, because the OIG resolves this matter on other grounds, it assumes, without deciding, that the complainant's actions constituted a protected disclosure under the Act.

[41] In case law interpreting the Act, the Merit Systems Protection Board has considered actions taken within several months of the protected disclosure to be close enough in time under the "knowledge/timing" test. *See generally*, *Inman v. Department of Veterans Affairs*, 112 M.S.P.R. 280, 283-284 (2009) (reassignment 15 months after

FOR OFFICIAL USE ONLY

This document remains the property of the Office of Inspector General and is provided to you for official use in accordance with your duties. This document may contain law enforcement sensitive information as well as be protected by the Privacy Act, 5 U.S.C. § 552a. Per DAO 207-10, do not disclose or disseminate this document or the information contained herein, or otherwise incorporate it into any other records system, without prior written permission from the Office of Inspector General. Public release will be determined by the Office of Inspector General under the terms of the Freedom of Information Act, 5 U.S.C. § 552, and the Privacy Act, 5 U.S.C. § 552a. Requests for copies of this report must be referred to the Office of Inspector General in accordance with DAO 207-10.

Although the complainant has established a *prima facie* case of retaliation, the agency has presented clear and convincing evidence that it would have taken the same actions in the absence of the complainant's disclosures. In this regard, management took personnel actions based in large part upon information that the complainant provided to [redacted] about [redacted] unauthorized access to the LInX database. This information, coupled with reports that the complainant had traveled to a foreign country without authorization while on extended leave, used an unauthorized thumb drive, and failed to protect the combinations to classified spaces, resulted in the initiation of an administrative inquiry that placed the complainant on fulltime telework, suspended [redacted] security clearance and government email account, and further delayed [redacted] deputation by USMS.

In addition to the strength of the evidence supporting the inquiry into the complainant's misconduct, the evidence does not demonstrate that [redacted] or [redacted] harbored retaliatory animus against the complainant for [redacted] disclosures. Rather, the evidence demonstrates that they made efforts to assist the complainant despite [redacted] job performance issues and the challenges that [redacted] had encountered in [redacted] new job position. Regarding the complainant's reports to [redacted] about the harassment of a [redacted] coworker, both [redacted] and the [redacted] coworker confirmed that [redacted] addressed the issue with the [redacted] coworker and determined that no further action was needed. Further, after the complainant raised [redacted] concerns about the computer searches to [redacted] in [redacted], [redacted] counseled the complainant and another agent on ITMD's computer search process. In addition, [redacted] also discussed the rationale behind ITMD's process with the complainant. And although [redacted] disputed that the complainant had reported concerns about computer searches directly to [redacted] in the [redacted], [redacted] was aware that the computer searches were an issue in the office at that time. Around that same time, [redacted] approved the complainant's application for special deputation on [redacted], despite the complainant's [redacted] the BAT. In addition, [redacted] took efforts to accommodate the complainant's request to transfer positions following the complainant's emails to [redacted] in [redacted].

The agency has also presented clear and convincing evidence that it would have taken the same personnel actions in the absence of the complainant's disclosure to OHRM. As discussed above, there is no evidence that either [redacted] or [redacted] were aware of the complainant's disclosures to OHRM in [redacted]. In addition, [redacted] contacted OHRM with [redacted] concerns about the complainant's performance on the BAT six days before the complainant contacted OHRM. Following [redacted] communication with OHRM, OHRM determined that the BAT should not have been included as a mandatory condition of employment on the position announcement under which the complainant was hired, but that the BAT could be included in the complainant's

---

disclosure); *Kalil v. Department of Agric.*, 96 M.S.P.R. 77, 85 (2004) (suspension proposed six months after disclosure).

FOR OFFICIAL USE ONLY

This document remains the property of the Office of Inspector General and is provided to you for official use in accordance with your duties. This document may contain law enforcement sensitive information as well as be protected by the Privacy Act, 5 U.S.C. § 552a. Per DAO 207-10, do not disclose or disseminate this document or the information contained herein, or otherwise incorporate it into any other records system, without prior written permission from the Office of Inspector General. Public release will be determined by the Office of Inspector General under the terms of the Freedom of Information Act, 5 U.S.C. § 552, and the Privacy Act, 5 U.S.C. § 552a. Requests for copies of this report must be referred to the Office of Inspector General in accordance with DAO 207-10.

performance plan. There is no evidence that decision to change the BAT from a mandatory requirement to a performance element was due to the complainant's disclosures to OHRM; rather, the evidence shows that these changes followed guidance that received from OHRM in response to own reports about the complainant's the BAT. Furthermore, even if or had known about the complainant's disclosures to OHRM in the , the evidence indicates that any disciplinary actions that management contemplated taking against the complainant were not due to complaint to OHRM, but rather, were due to the BAT. Moreover, despite the complainant's the BAT, nonetheless approved the complainant's application for special deputation to USMS for submission in . Following the submission of deputation application, factors such as the complainant's leave and evidence of misconduct resulted in the continued delay of the complainant's deputation, and thereby superseded any connection between the complainant's OHRM disclosure and management's actions in the .

For the reasons stated above, the evidence does not support the complainant's claim of whistleblower retaliation. The complainant established a prima facie case of retaliation through satisfying the "timing/knowledge" test. However, given the strength of the agency's evidence in support of its personnel actions, and the lack of evidence of retaliatory motive, the OIG found that the agency has established that it would have taken the same actions in the absence of the complainant's disclosures.

3. PPD-19

In addition to the protections afforded under the Act, Presidential Policy Directive 19 (PPD-19) prohibits retaliation against employees (1) serving in the intelligence community or (2) who are eligible for access to classified information for reporting fraud, waste, and abuse. Specifically, PPD-19 prohibits officers of executive agencies who have the authority to take action affecting an employee's eligibility for access to classified information from taking or failing to take action affecting an employee's eligibility for access to classified information in retaliation for making a protected disclosure.[42]

As the complainant alleged that suspended security clearance in retaliation for protected disclosures, this matter appears to fall under the purview of PPD-19. However, the OIG found that the evidence did not establish that or retaliated against the complainant, in part by suspending security clearance, due to protected disclosures. For

[42] Presidential Policy Directive/PPD-19, October 10, 2012.

FOR OFFICIAL USE ONLY

This document remains the property of the Office of Inspector General and is provided to you for official use in accordance with your duties. This document may contain law enforcement sensitive information as well as be protected by the Privacy Act, 5 U.S.C. § 552a. Per DAO 207-10, do not disclose or disseminate this document or the information contained herein, or otherwise incorporate it into any other records system, without prior written permission from the Office of Inspector General. Public release will be determined by the Office of Inspector General under the terms of the Freedom of Information Act, 5 U.S.C. § 552, and the Privacy Act, 5 U.S.C. § 552a. Requests for copies of this report must be referred to the Office of Inspector General in accordance with DAO 207-10.

the same reasons that the OIG found that [redacted] and [redacted] actions did not constitute a violation of the Act, the OIG also found that their actions did not violate PPD-19.

4. Agency's Personnel Actions

Although the OIG found that the Agency has presented clear and convincing evidence that the personnel actions it took in [redacted] were not in retaliation for the complainant's previous disclosures, the nature of some of the personnel actions taken may have violated DOC's IT policy. The DOC Commerce Information Technology Requirement (CITR) provides, in relevant part:

> Official DOC work and digital communications (e.g., email) must be carried out using authorized DOC IT accounts. Official DOC communications are defined as any transfer of signs, writing, images, data, or intelligence for the purpose of supporting a DOC mission or objective. Use of personal accounts for official work or communications is prohibited.[43]

As the complainant's access to [redacted] DOC email account was suspended during OSY's investigation, [redacted] instructed the complainant to use [redacted] personal email account to send status updates.[44] The complainant therefore used [redacted] personal email account to send about thirty work-related emails between [redacted], and [redacted].[45] As the only exceptions to DOC's IT policy are in cases of emergency, the evidence indicates that [redacted] instructions led the complainant to violate DOC policy.

III. Conclusion

Based on the above, the OIG found that there is insufficient evidence to support the allegations that [redacted] and [redacted] delayed the complainant's special deputation or initiated an administrative investigation due to disclosures the complainant made to various DOC officials between [redacted] and [redacted]. However, the evidence indicates that [redacted] caused the complainant to violate DOC IT policy by directing [redacted] to send work-related emails from [redacted] personal email account while [redacted] DOC email account was suspended during the OSY investigation.

---

[43] Department of Commerce, *Commerce Information Technology Requirement,* CITR-022 para. 6.6 (Apr. 15, 2014), available at https://connection.commerce.gov/sites/connection.commerce.gov/files/media/files/2014/citr-022_access_and_use.pdf.

[44] CMS entry No. 23 at 11.

[45] CMS entry No. 14 at 6.

FOR OFFICIAL USE ONLY

This document remains the property of the Office of Inspector General and is provided to you for official use in accordance with your duties. This document may contain law enforcement sensitive information as well as be protected by the Privacy Act, 5 U.S.C. § 552a. Per DAO 207-10, do not disclose or disseminate this document or the information contained herein, or otherwise incorporate it into any other records system, without prior written permission from the Office of Inspector General. Public release will be determined by the Office of Inspector General under the terms of the Freedom of Information Act, 5 U.S.C. § 552, and the Privacy Act, 5 U.S.C. § 552a. Requests for copies of this report must be referred to the Office of Inspector General in accordance with DAO 207-10.

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

November 19, 2018

INFORMATION MEMORANDUM FOR SECRETARY ROSS

FROM: Peggy E. Gustafson
Inspector General

SUBJECT: Request for Information Pursuant to the Inspector General Act of 1978, as Amended.

This request for information is in anticipation of the Office of Inspector General (OIG) opening a fuller review of the Investigations and Threat Management Division (ITMD) and its associated components.

In the Department's Fiscal Year 2018 Congressional Submission, the Office of Security (OSY) requested a funding increase of $5,000,000 and 20 full-time equivalent for the expansion of ITMD.[1] The Program Justification stated:

> ITMD cross-cuts all Commerce operating units in order to detect critical threats to the Department's U.S. economic advancement mission, and is the sole U.S. Government agency with this focus. The program's investigative findings directly inform key decision-makers (including senior U.S. Government and Secretarial officials) and stakeholders (NSS, ODNI, DOJ) about serious threats to national security or public safety, and enable OSY to target and refine its security services against rapidly emerging threats which would have remained unidentified by other government agencies. The program fulfills U.S. national strategic requirements involving counterintelligence, transnational organized crime, and counterterrorism.

Further, Department Administration Order 207-11, Official Credential and Badge, notes that special agents within OSY may be "deputized for mission-critical threat and counter-intelligence functions."

---

[1] FY 2018 Congressional Submission, *available at* http://www.osec.doc.gov/bmi/budget/FY18CBJ/DM_CJ_2018_Master_with_pagination_OB_revision_05_22_17.pdf.

Given this and other information that has been brought to the attention of the OIG, the OIG requests that you provide responses to the following, with relevant documents, by Friday, November 30, 2018.

1. Please explain the mission of ITMD, including any change in the mission historically and any possible planned changes in the mission.

2. Please explain how ITMD carries out the mission described in your response to the first item. Please include all policies and procedures, formal or informal, followed in carrying out such approach. Please also include any handbook or other relevant documents. If there are no documents relevant to this request, please state so.

3. Please explain the legal authority, statutory, regulatory, or otherwise, under which ITMD undertakes the mission described and documented within your response to the first item above.

4. Please describe whether ITMD considers itself a law enforcement entity, and whether and how ITMD associates, cooperates, or consults with any law enforcement entity.

5. Please describe whether ITMD considers itself a member of the Intelligence Community, and whether and how ITMD associates, cooperates, or consults with any member of the Intelligence Community.

6. Please describe ITMD's casework, including any involvement outside of Department of Commerce properties and any involvement in matters associated with persons who are not Department of Commerce employees.

7. Other than the Department of Commerce OIG, which has full oversight authority, please describe any oversight of ITMD, including oversight outside of OSY. This should include any policies and procedures relevant to oversight.

In addition, you may also produce any additional documentation or information deemed relevant to this request for information.

The Inspector General Act of 1978 guarantees the Office of Inspector General (OIG) timely access to "all records, reports, audits, reviews, documents, papers,

recommendations or other materials" available to the Department,[2] and authorizes the IG to "make such investigations and reports relating to the administration of programs and operations of [the Department] as are, in the judgment of the Inspector General, necessary or desirable[.]"[3] Department Administrative Order 213-2, § 4.03 states that "it is Departmental policy that all employees fully cooperate with the OIG," and that "Department officials shall make every effort to assist the OIG in achieving the objective of effective inspections and evaluations." Similarly, Department Organizational Order 10-13, § 4.01 states that "[t]he officers and employees of the Department shall cooperate fully with the officials and employees of the OIG and shall provide such information, assistance, and support without delay as is needed for the OIG to properly carry out the provisions of the [Inspector General] Act [of 1978]."

If you have any questions or need additional information, please contact me at (202) 482-4661.

---

[2] 5 U.S.C. App. § 6(a)(1)(A).
[3] *Id.* § 6(a)(2).

UNITED STATES DEPARTMENT OF COMMERCE
Chief Financial Officer
Assistant Secretary for Administration
Washington, D.C. 20230

DEC 2 0 2018

MEMORANDUM FOR THE INSPECTOR GENERAL

FROM: Lisa Casias
Acting Chief Financial Officer/Assistant Secretary for Administration, and Deputy Assistant Secretary for Administration

SUBJECT: Response to Request for Information Pursuant to the Inspector General Act of 1978, as Amended

This memorandum serves to transmit materials responsive to your request, provided to Secretary Ross, on November 19, 2018 seeking information related to the Office of Security's Investigations and Threat Management Division.

Attached you will find responses to the enumerated questions; however, portions of the requested materials and context associated with them are best provided via a classified briefing in a controlled environment attended by those holding appropriate clearance levels.

If you have any questions or should you or a member of your staff require a classified briefing, please contact Richard Townsend, Director for Security at (202) 482-4371.

ATTACHMENT

1. Response for Information Pursuant to the Inspector General Act of 1978, as Amended

1. Please explain the mission of ITMD, including any change in the mission historically and any possible planned changes in the mission.

The mission of the Department of Commerce is to promote the economic advancement of the United States. 15 U.S.C. § 1512 and Department Organization Order (DOO) 1-1, which is essential to U.S. national security. Commerce's Office of Security (OSY) performs Department-wide functions to ensure this mission. In furtherance of these functions, OSY is chartered to identify and assess any threat to the Department's mission or activities, conduct investigations, and protect personnel, property, and assets. DOO 20-6. The Investigations and Threat Management Division (ITMD) identifies, assesses and protects against threats to the Department's mission-critical assets – those 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 (Supplemental Letter – Attachment 1). ITMD is also designated under DOO 20-6 as being responsible for ensuring the effective implementation of Executive Order (EO) 13587 (Insider Threat) and currently serves as the Department's Federal Senior Intelligence Coordinator pursuant to a 2017 designation by the Deputy Secretary.

In FY18, the ITMD budget, which was historically funded from the Working Capital Fund (WCF), was moved to Salary & Expense (S&E) appropriated funds consistent with language in the final Congressional appropriation. Attached are printouts (Attachment 2) of the FY18 final operating budgets as distributed by the Office of Financial Management which serve to illustrate the move. "OSY – FY 2018 WCF Final Operating Budget" has a WCF project number 0156 that shows a budget of "0M" in FY18 with no funded positions (i.e. FTE). In FY17, the WCF budget was $3.736M and supported 15 FTE. Conversely, "OSY – FY 2018 SE Final Operating Budget" has S&E project number 6116 that shows an S&E budget of "4.798M" in FY18 with 20 funded positions (i.e. FTE). In FY17, the S&E budget was $0M and supported no funded positions. With the WCF to S&E move and added resources from the Congressional appropriation, OSY was targeting an FY18 end-state operating budget of $5M and 20 FTE. However, there were back-end overhead adjustments that resulted in the final operating budget being reduced to $4.798M for OSY expenditure. Given the timing of the appropriation and the move, the FY19 operating request utilizing S&E funds remained flat.

2. Please explain how ITMD carries out the mission described in your response to the first item. Please include all policies and procedures, formal or informal, followed in carrying out such approach. Please also include any handbook or other relevant documents. If there are no documents relevant to this request, please state so.

Because of its protective stance, when possible ITMD's goal is to prevent or mitigate the occurrence of a mission-critical threat, and therefore acts to proactively identify unreported or unrecognized threats with action areas corresponding to the Department's Strategic Plan. ITMD also commences or coordinates investigations and operations to protect against recognized mission-critical threats, and thus receives reporting and referrals from other individuals and entities involving matters with a nexus to its primary mission. ITMD staff conduct investigative activities that may involve administrative or law enforcement techniques, are tiered and structured for efficiency, and prioritized by degree of known threat or risk. Threats can trigger concurrent or final threat management actions, which include ensuring stakeholder awareness of potential threats to their equities, coordinating or executing other threat management or law enforcement measures, and/or informing U.S. Government or Departmental strategies, policies and decision-makers. Generally, Department policy pertaining to ITMD is described in the U.S. Department of Commerce, Manual of Security Policies and Procedures, December 2012,

Chapter 36, which is located at http://home.osec.doc.gov/osy/SecurityManual/Security%20Manual.pdf. Additional information is best made available through a briefing, if required.

In August 2018, ITMD obtained contractor support to produce a current Division Directives Manual (DDM) based on internal training materials, both draft and enacted Division directives, and external best practices. The DDM project is divided among mission, authority, resource management and inspections, administrative management, investigative and threat management activities, performance management, and special activities sections, and will memorialize from a policy/procedure perspective new and pre-existing formal and informal protocols. Investigative artifact templates, example policies, and an informal quick reference guide are attached (Attachment 3). In addition to the documents attached, we can also provide OIG with other draft documents, if required.

3. Please explain the legal authority, statutory, regulatory, or otherwise, under which ITMD undertakes the mission described and documented within your response to the first item above.

OSY/ITMD's primary mission is the protection of Department critical assets. Presidential Policy Directive (PPD) 21, *Critical Infrastructure Security and Resilience*, states, "All Federal department and agency heads are responsible for the identification, prioritization, assessment, remediation, and security of their respective internal critical infrastructure that supports primary mission essential functions." Pursuant to 5 U.S.C. § 301, through DOO 20-6, OSY has been delegated responsibility for:

> personnel security; industrial security; the safeguarding of classified and sensitive documents and information; protection of Department personnel, facilities, property, assets and activities; identification, assessment and mitigation of threats; security risk assessments; emergency actions and preparedness; physical security; executive protection; communications security; operations security; security education, awareness, and training; and compliance with security policies and procedures.

DOO 20-6, Section 3.01a.

The U.S. Marshals Service (USMS) is authorized to deputize Federal employees. 28 C.F.R. § 0.112 and USMS Policy Directive 17.11. USMS has issued deputations to OSY personnel for the purpose of protecting Department critical assets and the Secretary of Commerce. As stated in the USMS policy, deputized OSY personnel have Title 18 authority and are authorized to carryout federal law enforcement functions. USMS Policy Directive 17.11.

The Secretary of the Department of Homeland Security (DHS) may designate officers or agents to perform the law enforcement duties detailed in 40 U.S.C. § 1315(b) and *may* prescribe regulations regarding the protection of Federal property and persons on Federal property in consultation with the Administrator of the General Services Administration (GSA). *See also* 41 C.F.R. §§ 102-72.90. Under GSA regulations, an agency may request a security delegation from GSA. 41 C.F.R. § 102-72.95. OSY relies upon an October 27, 2018 five-year delegation from DHS to designate law enforcement personnel and protective security for three NIST sites: Gaithersburg Campus; Boulder Campus; and the Table Mountain Field Site and Radio Zone in Boulder, CO.

Additional authorities related to OSY and ITMD are listed within DOO 20-6, Section 4 and the U.S. Department of Commerce, Manual of Security Policies and Procedures, December 2012, Chapter 36, located at http://home.osec.doc.gov/osy/SecurityManual/Security%20Manual.pdf.

4. Please describe whether ITMD considers itself a law enforcement entity, and whether and how ITMD associates, cooperates, or consults with any law enforcement entity.

We are unaware of any government-wide definition of "law enforcement entity." OSY is not statutorily defined as a law enforcement agency; however, the U.S. Government Accountability Office (GAO) has used the term "law enforcement component" in describing federal organizations without statutory authority which nonetheless perform law enforcement functions. Components of OSY do perform law enforcement functions in connection with the duty to protect the Department and pursuant to the authorities described in Question 3. As described in the following responses, ITMD associates, cooperates, and consults with federal, state, local, military, and specialized law enforcement counterparts to obtain and refer investigative information, coordinate jurisdictional matters, and provide and receive assistance. ITMD is staffed with criminal investigators (Office of Personnel Management Job Series 1811) who conduct investigative activities in conformance with requirements that allow for the prosecution of crimes, and fall under the federal statutory definition of "law enforcement officer" (5 U.S.C. § 8401) in that the duties of these employees are primarily the investigation of individuals suspected of offenses against the criminal laws of the United States, or the protection of officials of the United States against threats to personal safety. Within ITMD's current caseload, many investigative matters involve interaction with stakeholder law enforcement entities, and if required the Division can provide additional information at the appropriate classification level to answer any questions about interactions involving specific cases. If this response differs from your intended question, please provide further clarification on your definition of "entity" and we will furnish additional information as necessary.

5. Please describe whether ITMD considers itself a member of the Intelligence Community, and whether and how ITMD associates, cooperates, or consults with any member of the Intelligence Community.

U.S. Intelligence Community (USIC) elements are specified by EO 12333 (EO 13470); the Department of Commerce is not a USIC element. ITMD associates, cooperates and consults with USIC elements to identify and manage threats to the Department, inform investigations, and ensure stakeholders are aware of threats identified by ITMD. Within ITMD's current caseload, many investigative matters involve association, cooperation or consultation with USIC elements. ITMD also associates, cooperates and consults with USIC elements as Federal Senior Intelligence Coordinator for various issues across the Department; the Division can provide additional information in a classified briefing to answer any questions about interactions involving specific matters, if required.

6. Please describe ITMD's casework, including any involvement outside of Department of Commerce properties and any involvement in matters associated with persons who are not Department of Commerce employees.

ITMD casework involves strategic or tactical level threats to the Department's critical assets, which can be of a national security and/or criminal nature. Although ITMD does have unclassified casework, or

casework at certain stages that is unclassified, additional information is best made available through a classified briefing, if necessary.

ITMD criminal investigators perform activities related to their official duties outside of Department properties and interact with persons who are not Department of Commerce employees (typically, such persons are subject matter experts, witnesses, victims or suspects). ITMD criminal investigators perform their duties in public areas, as well as areas subject to a reasonable expectation of privacy through consent, compulsory legal process, or other lawful means. Under special deputation, ITMD criminal investigators have Title 18 authority to perform federal law enforcement functions wherever the United States has law enforcement powers (USMS 17.11). Further, under 40 U.S.C. § 1315 delegation, ITMD agents have law enforcement authority to protect specified persons and properties, including duty in areas outside the property to the extent necessary to protect the property and persons on the property. Regardless of where ITMD is operating, staff act in pursuit of its mission to protect Department assets.

7. Other than the Department of Commerce OIG, which has full oversight authority, please describe any oversight of ITMD, including oversight outside of OSY. This should include any policies and procedures relevant to oversight.

Investigative activities are reviewed by supervisory criminal investigators through regular staff sessions; currently, most days have brief review sessions, with separate progress reviews for specific casework at other times based on threat and risk levels. The ITMD Assistant Director's work is overseen by the OSY Director through weekly meetings; the Department's Deputy Assistant Secretary for Administration (DASA) also maintains a bi-weekly meeting with the ITMD Assistant Director. On a recurring basis, overall caseload is assessed by a Risk Awareness Committee (framework attached – Attachment 4). ITMD criminal investigations accepted by the Department of Justice are overseen by corresponding US Attorney's Offices. Externally, ITMD was reviewed by Office of the National Counterintelligence Executive's National Counterintelligence and Security Center in 2011, 2013 and 2016, and was also reviewed by the National Insider Threat Task Force in 2014.

Redactions in Original Unless Otherwise Marked

UNITED STATES DEPARTMENT OF COMMERCE
Chief Financial Officer
Assistant Secretary for Administration
Washington, D.C. 20230

December 17, 2018

(b) (7)(F) Chief
Special Deputation Unit
Office of Security Programs, U.S. Marshals Service
2604 Jefferson Davis Highway
Alexandria, VA 22301

Chief (b) (7)

Pursuant to your request, please consider this letter as supplementation to our December 17, 2018 initial submission for special deputation. I authorize and concur with participation in the Special Deputation Program and certify that he is not the subject of any internal investigation.

Authority to Provide Security for Department of Commerce Critical Assets

The mission of the Department of Commerce is to promote the economic advancement of the United States (15 USC 1512, Department Organization Order 1-1), and the President's most recent National Security Strategy (December 2017) emphasizes the extreme significance of U.S. economic advancement in relation to U.S. national security. Commerce's Office of Security (OSY) performs Department-wide functions to ensure this mission; in furtherance of these functions, OSY is chartered to identify and assess any threat to the Department's mission or activities, conduct investigations, and protect personnel, property, and assets (Department Organization Order 20-6). The Director for Security is authorized to serve as the Department's liaison with agencies of federal, state, and local government for security matters, including obtaining special deputation from the U.S. Marshals Service for the authorization to carry firearms and make arrests in order to carry out such functions (DOO 20-6). The Director may also re-delegate his authority to designated personnel in OSY (DOO 20-6).

OSY maintains a classified inventory of the Department's critical assets, which are defined as activities or items which if compromised would cause significant damage to the U.S. Government's ability to function, U.S. economic advancement, or Departmental functions in support of these concerns. From time to time, this 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.

Authority to Protect the Secretary of Commerce

The Director for Security is responsible for assessing any threat to the Department's mission, and protecting the Department's personnel, facilities, property, assets, and activities (Department Organization Order (DOO) 20-6). The Department may use appropriated funds to protect an agency official when the Department determines that it

has a legitimate concern for the safety of the official and where the functioning of the Department may be impaired by danger to the official (54 Comp. Gen. 624 (1975)). The Director for Security is authorized to serve as the Department's liaison with agencies of federal, state, and local government for security and executive protection matters, including obtaining special deputation from the U.S. Marshals Service for the authorization to carry firearms and make arrests in order to carry out such functions (DOO 20-6). The Director may also re-delegate his authority to designated personnel in OSY (DOO 20-6).

OSY maintains a Principal Vulnerability Assessment regarding the Secretary of Commerce, which documents security concerns involving the Secretary sufficient to merit personal protective coverage in order to ensure the continued functioning of the Department.

Job Series and Title

began full time employment with the Office of Security on his official position description states that incumbents in his category (Office of Personnel Management job classification standards 1811 series – Criminal Investigator/Mission-Critical Threats) develop proactive threat identification, assessment, and management functions, and planning, conduct, and presentation of sensitive and complex investigations involving alleged or suspected violations of Federal criminal laws and regulations, including strategic investigations involving national security threats. receives special retirement coverage for federal law enforcement officers (5 USC 8412(d)), which is only provided to incumbents who occupy rigorous positions and whose primary duties are "investigating, apprehending, or detaining individuals suspected or convicted of offenses against the United States or protecting the personal safety of United States officials" (5 CFR 842.803). Employees assigned law enforcement duties and responsibilities are issued credentials with the working title of "Special Agent" (Department Administrative Order 207-11); serves as a Special Agent in the Investigations and Threat Management Division.

Experience and Training

All Special Agents assigned to OSY's Investigations and Threat Management Division are required to complete Basic Agent Training (which includes international security issues and national security interests; economic, technological, and environmental theory and policy; Constitutional law and the laws of arrest, search and seizure; federal criminal law and procedure; advanced investigative techniques; ethics; operations security; and control tactics and first aid instruction). Additionally, relevant law enforcement training also includes graduation from the Federal Law Enforcement

Special deputation to bear firearms and exercise arrest authority while **"providing security for Department of Commerce critical assets and protection for the Secretary"** is required in order to: 1) protect critical assets and the Secretary of Commerce, as described in this document; 2) ensure assigned special agents can protect themselves and others from danger; 3) protect evidence from destruction; and 4) ensure an interim Federal presence before other duly appointed investigative and law enforcement agencies can assume any related responsibilities. USMS special deputation will ensure that OSY has appropriate legal authority to act as necessary when other authorities to investigate, bear firearms, or make arrests are met in various contexts and under evolving circumstances.

Please contact me at (202) 482-3715 if you require further information. Thank you for your time and consideration in this matter.

Sincerely,

(b) (7)(E) [redacted]
Assistant Director
Investigations and Threat Management Division
Office of Security
U.S. Department of Commerce

SALARIES AND EXPENSES
OFFICE OF SECURITY
INVESTIGATIONS AND THREAT MANAGEMENT DIVISION (6116000/1104)
FY 2018 FINAL OPERATING BUDGET
(Dollar Amounts In Thousands)

		A	N=SUM(C:M)	O	P	R	S	T	U	V=SUM(N:U)
		FY 2017 FINAL BUDGET	FY 2018 DRAFT BUDGET	FY 2018 FINAL ATBs	FY 2018 FINAL REORG	FY 2018 FINAL SALARY LAPSE	FY 2018 FINAL OC ADJ.	FY 2018 FINAL OSFM ADJ.	FY 2018 FINAL PROGRAM INC / RECISSION	FY 2018 FINAL BUDGET
FTE	POSITIONS	0							20	20
1101	FULL TIME PERMANENT	0				(703)			2,379	1,676
1152	CASH AWARDS	0							25	25
1170	OVERTIME - REGULAR	0							469	469
1211	WORKER'S COMPENSATION	0							8	8
1231	TRANSIT BENEFITS	0						(30)	30	0
1200	BENEFITS	0				(366)			1,238	872
	TOTAL PAYROLL	0	0	0	0	(1,069)	0	(30)	4,149	3,050
1300	UNEMP COMP & VERA/VSIP	0								0
2111	DOMESTIC TRAVEL	0							144	144
2112	FOREIGN TRAVEL	0							0	0
2200	TRANS. OF THINGS	0							33	33
2319	RENT PAYMENTS TO GSA	0						(88)	88	0
2300	TELEPHONE & UTILITIES	0						(23)	40	17
2410	PRINTING	0							10	10
2500	OTHER SERVICES	0				1,069			81	1,150
2530	TRAINING - ALL	0							143	143
2580	WCF CHARGES	0						(61)	100	39
2595	CHARGES FM OTH AGENCIES	0							75	75
2600	SUPPLIES	0							38	38
3124	CAPITALIZED EQUIPMENT	0							0	0
3144	NON-CAP. EQUIPMENT	0							98	98
	TOTAL OTHER COSTS	0		0	0	1,069	0	(172)	851	1,748
	TOTAL OFFICE COSTS	0	0	0	0	(0)	0	(202)	5,000	4,798

WORKING CAPITAL FUND
OFFICE OF SECURITY
INVESTIGATIONS AND THREAT MANAGEMENT DIVISION - 0156000/1104
FY 2018 FINAL OPERATING BUDGET
(Dollar Amounts In Thousands)

05/15/2018

		A	N=SUM(C:M)	O	P	Q	R	S	T	U	V=SUM(N:U)
		FY 2017 FINAL BUDGET	FY 2018 DRAFT BUDGET	FY 2018 FINAL ATBs	FY 2018 FINAL REORG	FY 2018 FINAL MOUs	FY 2018 FINAL SALARY LAPSE	FY 2018 FINAL OC ADJ.	FY 2018 FINAL OSFM ADJ.	FY 2018 FINAL PROGRAM INC / RECISSION	FY 2018 FINAL BUDGET
FTE	POSITIONS	15	14		(14)						0
1101	FULL TIME PERMANENT	1,633	1,677		(1,677)						0
1152	CASH AWARDS	15	24		(24)						0
1170	OVERTIME - REGULAR	226	360		(360)						0
1211	WORKER'S COMPENSATION	25	8		(8)						0
1231	TRANSIT BENEFITS	22	30		(30)						0
1200	BENEFITS	912	872		(872)						0
	TOTAL PAYROLL	2,833	2,971	0	(2,971)	0	0	0	0	0	0
1300	UNEMP COMP & VERA/VSIP	0	0								0
2111	DOMESTIC TRAVEL	36	37		(37)						0
2112	FOREIGN TRAVEL	0	0								0
2200	TRANS. OF THINGS	22	22		(22)						0
2319	RENT PAYMENTS TO GSA	85	88		(88)						0
2300	TELEPHONE & UTILITIES	40	40		(40)						0
2410	PRINTING	1	1		(1)						0
2500	OTHER SERVICES	23	26		(26)						0
2530	TRAINING - ALL	7	23		(23)						0
2580	WCF CHARGES	0	0								0
2595	CHARGES FM OTH AGENCIES	80	86		(86)						0
2600	SUPPLIES	8	10		(10)						0
3124	CAPITALIZED EQUIPMENT	0	0								0
3144	NON-CAP. EQUIPMENT	17	28		(28)						0
	TOTAL OTHER COSTS	319	361	0	(361)	0	0	0	0	0	0
	TOTAL OFFICE COSTS	3,152	3,332	0	(3,332)	0	0	0	0	0	0
9000	EXP FROM WCF INTRAFUND	601	555								0
	SUBTOTAL	3,753	3,887	0	(3,332)	0	0	0	0	0	0
9000	REVENUE TO WCF INTRAFUND	(17)	(22)								0
	TOTAL COST	3,736	3,866	0	(3,332)	0	0	0	0	0	0

U.S. DEPARTMENT OF COMMERCE
OFFICE OF SECURITY

SPECIAL AGENT DIRECTIVE

Effective Date: 07/01/2014 DRAFT

REFERENCES:

5 USC 301-302
5 USC 3345-3347
5 USC 8336
5 USC 8401
18 USC 922
18 USC 3041
18 USC 3500
22 USC 2291
22 USC 3927
22 USC 4802
22 USC 4805
28 USC 566
USM-3A/B
HR 3839
Vienna Convention on Consular Relations (1963)
28 CFR 0.112
EO 13242
USMSD 17.11
DOO 1-1
DOO 20-6
DOO 207-11
DAO 202-958
FLETC Legal Division Handbook (2010)

Attach # 3
Ref Q 2

PURPOSE: To define organization, authorized activities, and standards of service for all Office of Security (OSY) employees designated by the Director as Special Agents.

I. **Mission.** The Department of Commerce (DOC) is responsible for developing, fostering and promoting US economic advancement. OSY performs Department-wide functions aimed at reducing DOC's security risk.

A. **OSY Charter.** Department Organizational Order 20-6 (DOO 20-6) charters OSY to identify and assess any threat to the Department's mission or activities; protect personnel, property and assets; and serve as the Department's liaison with other agencies for protective and counterintelligence matters.

B. **Law Enforcement Capability.** Pursuant to federal statute, federal case law and Department of Justice legal opinions, the prevention of criminal offenses is an intrinsic function of law enforcement.

II. **Special Agent Program.** Special Agents provide, supervise or manage security services that require law enforcement authority to primarily prevent criminal offenses as authorized by DOO 20-6, Sections

2.03 and 3(b). OSY operates a Special Agent Program (SAP) for administering its law enforcement authorities and appointments; ensuring the qualifications, competency and integrity of appointed Agents; and regulating its law enforcement activities.

A. **Program Management.** Due to OSY investigative authority requirements and as the counterpart to the United States Marshals Service (USMS) Assistant Director for Investigations with responsibility for the Special Deputation Program (USMS-SDP), the Investigations & Threat Management Division Assistant Director (AD, ITMD) serves as the OSY Special Agent Program Manager (SAPM). In this capacity, the SAPM will:

1. Execute the provisions of DOO 20-6, Section 4.01(a), with respect to SAP matters.

   a. Secure, maintain and develop law enforcement authorities necessary or beneficial for accomplishing OSY's mission, including but not limited to the USMS-SDP.

   b. Continue to serve as the "appropriate Federal Official" cited on USM Form 3 for overall USMS-SDP administration, and perform an identical role for all other OSY law enforcement authorities.

   c. Establish and implement policies to effectively regulate OSY law enforcement appointments and activities.

   d. Designate qualified instructors and develop or coordinate general training requirements and curricula for OSY Special Agents.

   e. Perform compliance inspections or inquiries in accordance with this Directive.

   f. Maintain records which accurately document OSY law enforcement authorities, appointments and activities.

2. Execute the provisions of DAO 207-11, Section 5.05, with respect to credentialed OSY Special Agents.

3. Represent OSY with internal and external entities for SAP-related matters.

4. Delegate duties as necessary to ensure proper Program administration.

5. Prepare an annual report for the Director that summarizes SAP activities over the most recent fiscal year.

III. **Organization.** Special Agents may be employed to conduct investigations, perform protection, or oversee the planning and execution of either function.

A. **Immediate Office of the Director:** As eligible and with the concurrence of the Chief Financial Officer & Assistant Secretary for Administration, the Director and Deputy Director for Security may be appointed as Special Agents in order to perform law enforcement functions pursuant to DOO 20-6, Section 4.01(a).

B. **Investigations:** Agents who have been appointed on a full-time basis to ITMD pursuant to DOO 20-6, Section 5.02 to conduct investigations that identify, assess, prevent or mitigate critical threats to the Department's mission or activities.

C. **Protection:** Agents who have been appointed on a full-time basis to the Executive Security Protection Division (ESPD) pursuant to DOO 20-6, Section 5.01(c) to provide protection for the Secretary of Commerce.

D. **Managers and Supervisors:** ITMD and ESPD managers and supervisors who are directly responsible for planning and executing investigative functions pursuant to DOO 20-6, Section 5.02, or dignitary protection functions pursuant to DOO 20-6, Section 5.01(c) on a full-time basis.

IV. **Responsibilities and Chain of Command.** In order to effectively ensure the qualifications, competency and integrity of appointed Agents and regulate OSY law enforcement activities, the following roles are established:

A. **Director and Deputy Director for Security.** Pursuant to DOO 20-6, the Director maintains general oversight of and accountability for OSY's responsibilities and functions, with support as necessary from the Deputy Director.

B. **Special Agent Program Manager.** The SAPM provides technical oversight for law enforcement duties under the Office of Special Deputy Marshal (or for any other OSY law enforcement authority) for all lawful orders issued under the authority of the United States (US), to specifically include orders issued by the Director and Deputy Director for Security not inconsistent therewith.

C. **Managers and Supervisors.** Managers are responsible for planning and executing law enforcement functions and supervising subordinate employees that have been granted law enforcement powers, but may delegate these duties as necessary to supervisors or team leads while retaining final approval authority.

D. **Agents.** Agents are appointed by the Director and are responsible for fully complying with the policies and procedures contained in this Directive. When necessary, Agents will confer with their chain of command, beginning with their team leader or supervisor, for matters not explicitly addressed in this Directive.

E. **Augmentation.** Under exigent circumstances, Agents who are temporarily assigned to assist a different function fall under the on-scene command of that function's supervisor or their designee for all collateral duties.

1. Agents must hold authorities compatible with the duties of their temporary assignment.

2. Assigned Agents must comply with policies and guidelines for the function of which they are augmenting, as well as their own Division-specific policies and guidelines.

3. ITMD Agents assigned to a task force or special assignment under the control of another government agency must obtain separate authority to perform any law enforcement function outside the scope of OSY's authorities, and will be supervised by such agency's personnel for work that is the exclusive jurisdiction of that agency.

V. **Qualifications for Service.** In order to be eligible for appointment and maintain status as a Special Agent, personnel must:

A. Be a US citizen employed on a full-time basis by OSY, be properly classified in an 1811 or 0080 Office of Personnel Management job series, and fall under an official position description wherein the primary purpose of the position involves performing duties specified in DOO 20-6, Sections 4.01(a), 5.01(c) or 5.02.

B. Have not been convicted of a crime involving domestic violence, as defined in 18 USC 922.

C. Initially, possess 1 year of full-time law enforcement experience prior to OSY employment with a US federal agency that was empowered with general arrest authority.

1. Prior to appointment by the Director, if an Agent candidate has had a break in law enforcement service for 5 or more years the candidate is required to complete mandatory refresher training through the Federal Law Enforcement Training Center (FLETC) or an equivalent program.

D. Receive favorable adjudication for a Top Secret security clearance.

E. Possess a valid state driver's license.

F. Receive clearance from the Federal Occupational Health Service for service in the 1811 job series and/or under a position covered by 5 USC 8336 retirement, and maintain a basic level of physical fitness which is subject to examination for continued service as defined in DAO 202-958.

G. Initially, graduate from a FLETC basic law enforcement training program (or a substantially equivalent basic law enforcement training program that was conducted by another US federal agency and has been evaluated and approved by the SAPM).

H. Complete any other course of instruction required by the USMS-SDP or equivalent authority.

I. Complete required OSY Special Agent Orientation Training.

1. At minimum, Agents will receive SAPM-approved initial instruction on DOC and OSY missions; threats to DOC; OSY authorities and regulating directives; elements of selected criminal offenses; chain of custody for evidence and property; an overview of high liability skills (use of force, mechanics of arrest, first aid, physical countermeasures, firearms familiarization, and non-emergency vehicle operations); operations security; agent safety; law enforcement ethics; and flying while armed requirements.

a. During initial instruction, Agents will be tested on constitutional laws of arrest, search and seizure and federal criminal procedure. Failure to achieve a passing score in constitutional law will result in the Agent attending FLETC's Continuing Legal Education Program, while failure to achieve a passing score in federal criminal procedure will result in the Agent attending the US Attorney's Office New Agent Orientation.

J. Review and certify compliance with this Directive and any Appendices, including Use of Force policy.

K. Demonstrate proficiency with OSY issued weapons.

L. Initially, submit the USM-3A Form (or its equivalent with respect to another type of law enforcement authority) to the SAPM through their manager; the SAPM may require additional documentation to evaluate whether a candidate meets standards. After review, the SAPM will provide a record to the Director regarding the candidate's qualifications for service.

VI. Fitness for Duty. Special Agents must be of good moral character and prepared to fully discharge the functions of a federal law enforcement officer.

A. **Standards of Conduct.** Agents will act on and off duty in a manner befitting representation of OSY and Federal law enforcement, and shall obey all applicable federal, state and local laws while conducting personal affairs.

1. Operations Security. Agents are prohibited from providing to any person who does not have a clear and official need to know information that could be directly used to impede or compromise the integrity of investigative, law enforcement or protective activities conducted by OSY or another government agency.

a. When in doubt, in the absence of specific policy Agents are required to consult with their supervisor prior to release of information that may pose an operations security concern.

2. Unethical Gain. Agents may not use their official position to:

a. Avoid the consequences of illegal acts.

b. For personal or financial gain for themselves or others, except through official programs that are available to any law enforcement officer and require nothing more than the Agent's monetary consideration.

c. In connection with representation, testimonials or advertisements for any organization, commodity, or commercial enterprise, without the Director's written approval.

3. Ill Repute. Agents will not participate in any incident involving moral turpitude that impairs their ability to perform as federal law enforcement officers or causes OSY to be brought into ill repute. Except as necessary in the performance of official duties or where unavoidable because of family relationships, Agents will avoid regular or continuous association with persons whom they know, or should reasonably know, are under criminal investigation, indictment, or involved in present or past criminal behavior.

4. Potential Violations of Law or Regulation; Changes in Status. When an Agent has reason to believe that they have committed a violation of law, are the subject of a criminal investigation, or have had any criminal enforcement action taken against them by a government entity, they must immediately notify their supervisor of the circumstances surrounding the incident, investigation and/or enforcement action at issue.

5. Confirmation of Required Work-Related Conduct. Agents are subject to random drug testing in accordance with established Office of Human Resources Management (OHRM) policies, as well as annual driving and criminal history checks conducted by the SAPM.

B. **Post-Appointment Training Requirements.** After appointment by the Director, Agents will complete:

1. A formal Division-specific training program prescribed by their manager.

2. An annual SAPM-approved OSY Special Agent In-Service module (to include at minimum updated or refresher instruction on the topics addressed in Section V-F-1, Special Agent Orientation Training).

3. From time to time, any other mandatory training requirements prescribed by their supervisor.

VII. **Ability to Execute Law Enforcement Functions.** During official duty, Special Agents are required to maintain the ability to perform law enforcement functions or notify their supervisor regarding their inability to do so.

A. **Agent's Duty to Act.** Agents must notify their supervisor if they believe that they are unable to reasonably execute potential law enforcement functions for any reason, including but not limited to physical injury/illness, mental illness/exhaustion, use of controlled substances or other medicines, or when they are or might appear to be under the influence of alcohol.

B. **Supervisor's Duty to Act.** Supervisors may consider an Agent to be temporarily incapable of performing their duties if in the supervisor's judgment the Agent's ability to execute potential law enforcement functions appears to be impaired for any reason. If duty is expected, the supervisor should encourage the Agent to report to the Herbert C. Hoover Building Health Services Unit or other appropriate facility for assessment, treatment or referral.

1. Removal of Agent's Weapons, Credentials and Badge. Supervisors will remove an Agent's issued weapons, Special Agent credentials and badge whenever an Agent:

a. Is reassigned temporarily (for more than 90 days) to a position that does not require the execution of law enforcement duties.

b. No longer maintains eligibility for Special Agent status as described in Section V of this Directive, or reasonably appears to lack fitness for duty as described in Section VI of this Directive.

c. Reasonably appears to have failed to properly safeguard a weapon, credential or badge, or is the subject of a suspicion or allegation regarding improper handling, display or misuse of a weapon, credential or badge, including failure to comply with OSY policy, USMS deputation requirements (or equivalent authority), or FLETC range policies.

d. Is the subject of an administrative inquiry or criminal investigation, including but not limited to information indicating that the Agent is untrustworthy, presents an unacceptable security risk to the Department or US Government, or has reportedly engaged in threatening behavior that did or could have reasonably placed another person in fear or danger (except during the authorized use of force in accordance with this Directive or its Appendices).

e. Has been permanently reassigned to a position that is not responsible for executing law enforcement duties, including being removed from duty due to performance or conduct.

2. Removed Items. Removed items will be secured by the Agent's supervisor, unless the items are required by a duly authorized investigative agency during the course of an inquiry or investigation concerning the Agent.

3. Light Duty. Agents who meet criteria for Section VII-B-1-b may be placed on light duty to perform nonsworn Division functions wherein no law enforcement authority is exercised. Agents experiencing short term medical conditions that substantiate the criteria must submit to their supervisor a written statement from their physician which reflects that their participation would likely have a negative impact on their current medical condition; Agents must obtain written notification from their physician stating that the temporary medical condition no longer exists before being re-evaluated for return to full duty. While on light duty for any medical condition, supervisors will make reasonable accommodations for the employee in accordance with federal law and Department policy.

4. Director's Clearance Required. Agents who have had their weapons, credential and/or badge removed will have their duties and work assignments adjusted accordingly until remedial training or an investigation, as appropriate, have been completed by a person whose qualifications have been recognized by the Director, the investigation has been reviewed by the SAPM to ensure USMS-SDP (or other authority) reporting requirements, and the Director authorizes the Agent to resume law enforcement duties.

C. **Preparation for Duty.** Agents shall be prepared for assignment upon official duty, to include having prompt access to their issued credentials, handgun and communication device, unless otherwise authorized by Division policy or their supervisor.

VIII. **Exercise of Law Enforcement Authority.** Special Agents may perform law enforcement duties after completing Section V requirements, taking the oath of office, and receiving an appointment certificate from the Director.

A. **Accountability.** Agents are responsible for upholding the US Constitution, and exercising law enforcement authority in accordance with all applicable federal laws and DOC/OSY directives, including those issued through their chain of command.

1. When in doubt as to the legality or propriety of their activities, Agents will request guidance from their supervisor. For further clarification, supervisors will consult with the SAPM, who will formally liaise with the Office of General Counsel and/or other entities as appropriate.

B. **Terms of Authority.** Managers and supervisors are responsible for ensuring subordinate Agents know, understand, and operate within the terms of their granted law enforcement authority.

1. General Terms for All Agents (28 USC 566). Agents may take such enforcement measures as are necessary to carry out their Federal duties. Agents may make arrests without warrant if there are reasonable grounds to believe that a person has violated, is violating, or is about to violate federal law in their presence, and may carry firearms for personal protection. This authority is valid wherever the US has law enforcement powers for statutes of general application, including throughout the states, territories and possessions of the US; in areas under the special maritime and territorial jurisdiction of the US; and on US diplomatic soil.

a. Federal Duties for ITMD Agents. ITMD Agents may exercise these general terms whenever protecting the Department's critical assets, or protecting the Secretary of Commerce.

(1) DOC critical assets are defined as activities or items which if compromised would cause significant damage to US economic advancement, the US Government's ability to function, or Departmental functions in support of these concerns, and specifically includes intangible assets that are not contained in a DOC facility.

(2) Additionally, ITMD Agents may make warrantless arrests with probable cause for felonies not committed in their presence; seek and execute arrest and search warrants, and serve subpoenas and other legal writs; and engage in electronic surveillance.

b. Federal Duties for ESPD Agents. ESPD Agents may exercise these general terms whenever providing protection for the Secretary of Commerce (or designated successors in accordance with 5 USC 3345-3347 and Executive Order 13242).

(1) Providing protection is defined as personally conducting security advances for locations to which the Secretary will travel, escorting the Secretary during travel, and managing security threats that may arise during protective movements with the Secretary.

2. Special Terms. The SAPM is responsible for obtaining any special law enforcement authorities which have been acquired other than through the USMS-SDP, and providing managers with their terms of use.

C. **Exercise of Powers.** Law enforcement authority may be exercised only when Agents are acting under the direction (including written, verbal or delegated direction) of their manager or supervisor in the 1811 or 0080 job series.

1. Enforceability. Any action taken under OSY law enforcement authority must conform to requirements that allow for prosecution of crimes.

2. Preserving Mission Resources. Whenever reasonably possible and only without adversely affecting particular assignments, Agents will refer criminal offenses for appropriate disposition to other law enforcement agencies with primary jurisdiction in instances where enforcement measures taken by OSY would be detrimental to the overall execution of ITMD or ESPD Federal duties.

3. Reasonable Suspicion and Probable Cause. Agents must be able to articulate why they exercised law enforcement authorities. Agents may not use race or ethnicity to any degree in developing reasonable suspicion or probable cause, but may rely on race or ethnicity for specific suspect descriptions (exceptions apply for certain investigations conducted by ITMD Agents in accordance with Department of Justice guidelines).

   a. Establishing Reasonable Suspicion and Probable Cause. Agents may establish reasonable suspicion and probable cause through personal observation, the collective knowledge of other law enforcement officers, from information provided by an identified third party, or from information provided by an unidentified third party.

      (1) Information from Informants. Prior to taking action, Agents will carefully evaluate any information provided by an unidentified third party to include: how the source came to know the information, amount of detail provided, accurate predictions by the source of the suspect's future behavior, whether the information provided is against the source's interests, the timeliness of the information, how the information was delivered to the Agent, and above all whether and to what extent the Agent can corroborate the information. When possible, Agents will consult with the SAPM before taking law enforcement action that is based on information provided by an unidentified third party.

4. Searches and Seizures. Any Agent may conduct warrantless searches and seizures as a law enforcement officer when doing so is reasonably necessary to fulfill their protective responsibilities, in accordance with the specific terms of their law enforcement authority, this Directive, and the policies of their respective Division. Agents may seize any contraband or evidence of a crime that is discovered during a warrantless search, as well as seize persons with whom they have reasonable suspicion (as an investigative detention) or probable cause (as an arrest) to believe have violated, are violating, or are about to violate federal law in their presence. *Lawful Presence and Right of Access*. Agents must be lawfully present to conduct searches or seizures. For locations other than a public place, Agents must have consent, exigent circumstances, or a warrant to be lawfully present or gain access to persons and property. *No Private Agents*. No Agent may enlist a private person in an attempt to circumvent Fourth Amendment search and seizure requirements. *Warrants*. All potential searches or seizures that are anticipated to require a warrant or other legal process will be referred to the AD, ITMD.

   a. Warrantless Searches. Agents may conduct warrantless searches of abandoned property, for inventory purposes, during plain view, after obtaining consent, at security checkpoints, or under exigent circumstances; Agents may also frisk persons who are under investigative detention whom they reasonably suspect are armed and dangerous. *Scope*. All searches are limited to areas wherein the item(s) that Agents are searching for could be found. Inventory searches must have no investigative purpose, consent searches are governed by the person providing consent, and security checkpoint searches are limited to persons who begin the inspection process but appear to subsequently attempt to avoid inspection. Frisks are limited to the discovery of weapons that may harm the Agent or other persons. For all other searches, Agents must terminate a search when the evidence in question has been discovered, or when all possible locations where evidence could be present have been searched. *Safety*. All searches must be performed by at least 2 Agents together, unless compelling circumstances exist that demand an immediate search after due consideration for the safety of the Agent and others.

      (1) Abandoned Property. After advance approval from their supervisor, Agents may search premises and property wherein an expectation of privacy has been intentionally and voluntarily relinquished. *Prohibitions*.

Agents may not search abandoned property if the abandonment was caused by an illegality.

(2) Inventories. After informing their supervisor, Agents will inventory and document all property that enters into the lawful custody of OSY for safekeeping during the course of the Agent's duties after any searches have been conducted pursuant to other authorities. If possible, Agents should make every effort to immediately return valuable items to an identified owner. *Prohibitions*. Agents must exercise due care to avoid unnecessarily damaging items during an inventory, and may unlock items that are accompanied by an unlocking device but may not otherwise open locked items.

(3) Plain View. Wherever an Agent observes in plain view an item that they have probable cause to believe is immediately apparent as contraband or evidence of a crime, the item may be seized. *Prohibitions*. Agents may not take action that results in bringing items into their view that would otherwise be undetectable.

(4) Consent. Consent eliminates the requirement for a warrant or the need for probable cause. Agents may request verbal or written consent to search premises, property or persons from the person to be searched, or for premises or property a person or third party who shares common control. Consent must be voluntary without coercion or misrepresentation, and the person providing consent may revoke their consent at any time, or otherwise control the conditions of the search. Agents must obtain specific consent for any locked containers, and are prohibited from damaging property during a consent search. *Prohibitions*. Agents are not authorized to obtain consent from a minor, a person who appears to be under the influence of alcohol or a controlled substance, a person who appears to be mentally retarded, or any time more than 1 party has authority to give consent but another party with equal authority refuses to give consent. Agents may not make promises to persons as a condition to obtain their consent. When possible, Agents will consult with the SAPM before attempting to obtain consent.

(5) Inspections. Agents may continue the inspection of persons (and any property in the possession of such persons) that have already begun the security screening process but subsequently take action to avoid a required inspection. *Prohibitions*. Agents may not establish specific checkpoints for searching persons attending an event or accessing a Department facility to secure evidence of a particular crime.

(6) Frisking. Agents may conduct a pat down of the outer clothing of persons whom they reasonably suspect did, are or are about to violate federal law and are armed and dangerous. Agents may restrain persons prior to frisking, and remove any hard object they discover (for persons in heavy jackets, Agents may frisk underneath the jacket to avoid missing potential weapons). Container and vehicle frisks are permissible whenever an Agent has reasonable suspicion that the property is in the immediate control of the suspect and contains a weapon (for vehicles, only the passenger compartment and any unlocked containers therein may be frisked). *Prohibitions*. Agents may not use frisking to look for evidence of a crime, although while frisking they may seize objects which are immediately apparent as contraband or criminal evidence as long as no additional manipulation occurs.

(7) Exigent Circumstances. Agents may conduct a search that would otherwise require a warrant when they have probable cause to believe that they are acting to prevent the destruction of evidence, a suspect's escape, or the death or injury of a person for as long as these particular exigent circumstances exist. *Evidence Destruction*. Agents who can articulate that evidence of a crime is present at a specific location and is being, or will be, destroyed before a warrant can be obtained may search to prevent its immediate destruction, but must secure the scene and obtain a warrant to continue the search. *Emergencies*. Agents may search when an imminent risk of danger exists to the Agent or others; when a person is seriously injured; when preventing a suspect from escaping; or when in continuous pursuit of a fleeing felon from a public place. *Mobile Conveyances*. Agents may also search mobile conveyances (including any locked containers or compartments, regardless of ownership) if they have probable cause to believe that contraband or evidence of a crime is located within, and that the vehicle is readily mobile. *Prohibitions*. In no instance can an Agent create an exigency to enable a warrantless search.

b. Warrantless Seizures of Property. Agents will maintain chain of custody over seized property pursuant to a warrantless search (including inventory searches), provide a written receipt to persons from whom property has been seized, and promptly provide seized property to the ITMD Evidence & Property Custodian for storage until disposition in accordance with ITMD operating procedures. Agents encountering evidence that requires special identification or handling will defer collection to the ITMD Evidence & Property Custodian.

(1) Chain of Custody. When agents seize or otherwise handle seized property, they must affix or update documentation to the container in which the evidence is stored that memorializes who recovered the evidence, when and where it was found, where the evidence has been, and who has handled or (with respect to necessary tests) altered it. Also, Agents must take steps to protect seized property from unintentional alteration or damage. Agents may not reuse evidence collection, storage or testing materials.

c. Warrantless Seizures of Persons. Agents may approach any person who is entitled to terminate contact and leave at any time and engage in a consensual encounter, including asking questions, requesting (but not requiring) identification, and asking for consent to search or seize. *Investigative Detention*. Agents with reasonable suspicion that a person has violated, is violating, or is about to violate federal law in their presence may effect an investigative detention, using reasonable force if necessary; Agents may also use any legal justification for the stop even if they are investigating a different, more serious crime for which at present they lack reasonable suspicion. When effecting an investigative detention, Agents must identify themselves as a law enforcement officer (if possible by verbal declaration and display of their badge and/or credentials), confine their questions to those that would confirm or dispel their suspicion, use investigative techniques that are the least intrusive means reasonably available in a short period of time, and end the detention as soon as the purpose of the stop has been fulfilled. While performing an investigative detention, Agents may order occupants out of a vehicle, as well as restrain detainees when such persons display aggression or are suspected of being involved in a violent crime. *Arrest*. Agents with probable cause to believe that a person has violated, is violating or is about to violate federal law in their presence may effect an arrest after making known to the offender that they are being arrested; warrantless arrests of persons who are not in a public place require consent, exigent circumstances, or a warrant in order to gain access to the arrestee. *Safety*. All investigative detentions or arrests must be performed by at least 2 Agents together, unless compelling circumstances exist that demand an immediate seizure with due consideration for the safety of the

Agent and others. When practical, encounters with persons for the purpose of making an investigative detention or arrest must be communicated to a supervisor, or in the absence of a supervisor to another available law enforcement agency with jurisdiction.

(1) Search Incident to Arrest. After physically restraining an arrestee, Agents will perform without delay a search of the arrestee's person, and areas within the arrestee's immediate control (defined as slightly beyond the arrestee's arm's reach, and including searching the arrestee's personal property and opening any locked containers as necessary) at the place of arrest to secure any weapons, contraband or evidence present. *Vehicles*. If the person arrested was taken into custody from or immediately exiting a vehicle and Agents did not subsequently move the arrestee away from the vehicle, Agents may search areas within such an arrestee's immediate control (defined as the passenger compartment, and including opening any locked or unlocked containers as necessary, but not searching other occupants without separate justification). *Protective Sweeps*. Agents may also briefly look into areas immediately adjoining where the arrest took place, and if they have a reasonable suspicion that others are present who pose danger may conduct a protective sweep slightly beyond immediately adjacent areas to locate and detain such persons. *Minimizing Risk*. After conducting a search incident to arrest, Agents will move the arrestee to an inconspicuous location which limits avenues of escape while awaiting prisoner transport.

(2) Notifications. If unable to do so in advance, Agents will notify their supervisor after making an investigative detention or arrest as soon as practicable.

(3) Custodial Interrogation. Agents are not authorized to conduct a custodial interrogation without permission from the AD, ITMD.

(4) Criminal Complaint and Initial Appearance (18 USC 3041). Agents will request assistance from the USMS District in which the crime occurred (or any law enforcement agency with proper jurisdiction, if USMS assistance is unavailable) to assist in processing the arrestee and transporting them without unnecessary delay to the nearest US magistrate judge, US district court judge, or under exigent circumstances another statutorily empowered official. Agents will prepare a criminal complaint articulating probable cause for the arrest prior to taking the arrestee before an authorized official, and will sign the complaint under oath in the presence of the official.

(5) Warrant Service. If an arrest warrant is issued subsequent to the complaint, Agents will request USMS assistance for processing and incarceration.

(6) Arresting Juveniles. Agents who have arrested a juvenile (a person under the age of 18) must administer Miranda rights in words that a juvenile can understand, even if no questioning will take place, and must expeditiously take the arrestee before a US magistrate judge.

(7) Congressional Privilege. Generally, members of congress may not be arrested while Congress is in session and while attending, or going to and from, sessions of congress. However, members may be arrested for a felony or crime involving violence.

(8) Detention or Arrest of Foreign Nationals within the US. Pursuant to the Vienna Convention on Consular Relations, Agents detaining or arresting a foreign national (non-US citizen) will immediately inform the foreign national of their right to have their Government notified. If the foreign national claims to have diplomatic immunity, Agents will inform them that they will be detained until their identity and status have been verified. Verified foreign nationals with diplomatic immunity may not be arrested, but may be restrained or searched if they pose an immediate threat to safety.

5. Documentation. Agents are required to accurately and completely document all activities which involve the exercise of law enforcement authority. In order to fulfill discovery obligations (including Brady, Giglio and Jencks requirements), this includes but is not limited to:

   a. Testimonial evidence from the defendant, including any recorded or written statement made by the defendant that is relevant, as well as verbal statements made to a person the defendant knew was a government agent at the time the statement was made.

   b. Relevant documentary and physical evidence, including papers, photographs and records, whether or not obtained from the defendant.

   c. Relevant forensic evidence, including tests, reports and analyses.

   d. Any known exculpatory evidence.

   e. Any information that contradicts a witness or tends to make a witness less believable (including information specific to involved law enforcement officers), such as payment of money for testimony, character evidence of untruthfulness or bias, information that a witness has lied in an investigation, pending investigations of truthfulness or bias based upon a credible allegation, or findings of a lack of candor during an administrative inquiry.

   f. Any prior statements of a trial witness in possession of the government, including affidavits, notes that have been verified as accurate by a witness, recorded statements, close transcripts of witness testimony, and law enforcement reports of witness interviews.

6. Law Enforcement Activities in Foreign Countries. The SAPM will coordinate all law enforcement activities intended for execution in a foreign country with the Departments of State and Justice and DOC Office of General Counsel, except for executive protection assignments. Agents are required to coordinate with their supervisor prior to foreign travel for official or diplomatic designations.

   a. Obligations to the US Chief of Mission (22 USC 3927(b); 22 USC 4802; 22 USC 4805). Agents engaging in official US Government business in a foreign country shall keep the Chief of Mission (or the Deputy Chief of Mission, if so delegated) fully and currently informed of all activities in that country, and fully comply with all applicable directives from the Chief of Mission. Also, if the Chief of Mission believes that an OSY law enforcement activity conducted within his or her area of responsibility would significantly damage US interests abroad, he or she may suspend the activity pending prompt resolution of the matter by the Departments of State, Justice and Commerce. The role of the Chief of Mission does not include ordering law enforcement officers to take investigative or prosecutorial steps, and if Agents believe that exceptional circumstances create a conflict of interest in sharing information with the Chief of Mission they must immediately report their concern to the SAPM before withholding such information.

b. Interviews. Agents shall not interview, nor be present during interviews, of any US citizen or resident alien who is in the custody of any foreign government in a foreign country without the written consent of that person. When conducting interviews of subjects who are in the custody of a foreign government, Agents shall take reasonable measures to ensure the individual is aware that he or she is not in the custody of the US, and will administer Miranda warnings prior to questioning. Agents may not interview or be present during interviews of any US citizen or resident alien arrested by foreign authorities with respect to narcotic control efforts.

c. Searches. Agents shall not conduct independent searches or joint searches with foreign authorities of US citizens or resident aliens in a foreign country (or enlist foreign authorities to act as their agent) without probable cause.

d. Arrests. Agents will not directly effect an arrest in a foreign country, but with approval from the Chief of Mission may assist foreign officers who are effecting an arrest.

e. Observed Human Rights Abuses. If Agents observe foreign government officials engaged in human rights abuses, they will request that the officials stop the activity, depart the area, and report the incident to the Chief of Mission and SAPM.

7. Crimes Outside of OSY Law Enforcement Authority. If an Agent determines that a crime has occurred but is not enforceable within the scope of their Federal duties, they must as soon as practicable notify a law enforcement agency with proper jurisdiction, followed by a notification to their supervisor. Under truly exceptional circumstances in domestic or foreign locations, Agents may use discretion and take reasonable action to protect life, although such action does not create law enforcement authority and only provides civil protections.

a. Federal Law Enforcement Officer Good Samaritan's Act (HR 3839). Generally, federal law enforcement officers who intervene in purely state or local criminal offenses are outside their scope of employment. However, if the crime involves protecting an individual in their presence from a crime of violence, providing immediate assistance to an individual who has suffered or who is threatened with bodily harm, or preventing the escape of an individual whom the Agent reasonably believes has committed in their presence a crime of violence, an Agent occupying a covered law enforcement position pursuant to DAO 202-958 may take reasonable action, but must turn over responsibility to the first available law enforcement agency with proper jurisdiction.

b. Serious Crimes Against Persons Occurring in a Foreign Country (22 USC 2291). If an Agent is on official business outside of the geographic boundaries of the US and a serious crime against a person is occurring, an officer or employee of the US may take direct action to protect life or safety if exigent circumstances arise which are unanticipated and which pose an immediate threat to US officers or employees, officers or employees of a foreign government, or members of the public.

8. Criminal and Civil Liability. Agents are subject to criminal sanctions for conspiring to violate a person's civil rights, or for intentionally violating the civil rights of others under color of law. Agents are subject to civil remedies for committing a constitutional tort (violations of rights protected under the Fourth, Fifth or Eighth Amendments), or in some instances a tort under state law. Searches and arrests without probable cause, knowingly submitting a false or misleading affidavit, and excessive force or failing to intervene when observing excessive force are all constitutional torts that require Agents to show they had acted in an objectively reasonable manner and without violating established rights of which a reasonable law enforcement officer would have known;

state torts (such as trespass, theft, battery, false arrest or imprisonment, and intentional infliction of emotional distress) require Agents to show that they acted within their scope of employment.

IX. **Other Matters Associated with Exercise of Law Enforcement Authority.** Official representation, property issued specifically for law enforcement purposes, use of law enforcement sensitive information, rendering emergency medical aid, and reporting of actions taken under law enforcement authority are subject to SAP regulation.

A. **Official Representation.** Only OSY employees who have received an appointment certificate from the Director may represent themselves as Special Agents, possess credentials, and issue correspondence or display business cards bearing the "Department of Commerce Special Agent" title, badge or emblem.

1. Representation and correspondence may only be in the furtherance of official duties and in accordance with DAO 207-11 and applicable federal law.

2. Agents may not represent themselves as officials of an agency from which they derive delegated law enforcement authority, unless such representation is consistent with that agency's policies and procedures.

3. Agents will display a "Department of Commerce Special Agent" badge and/or credential:

a. While the Agent is performing official duties in order to verify Special Agent status, unless the Agent is performing a covert assignment and such duty is documented by their supervisor prior to deployment;

b. Before, during, or as soon as practical after performing a law enforcement action requiring use of force, to include investigative detention or arrest; or

c. In conjunction with any public showing of a firearm, or during carriage of a firearm when the Agent must verify law enforcement status.

B. **Property Issued for Law Enforcement Purposes.** Agents are required to be familiar with the use of all property issued to them by OSY that has been identified by managers as being specifically for law enforcement purposes, and must retain individual control of, reasonably safeguard, and account for all such property. OSY issued property is subject to inspection by managers and/or supervisors at any time.

C. **Law Enforcement Sensitive Information.** Agents may only disclose information originating within OSY designated as "law enforcement sensitive" to authorized members of other law enforcement agencies that have a reasonable need to know, unless the Director has expressly approved dissemination. Agents receiving materials designated as "law enforcement sensitive" originating from another agency may only disclose such information to authorized members of other law enforcement agencies with a reasonable need to know, provided the originating agency has authorized dissemination.

D. **Rendering Emergency Medical Aid.** Agents are not required to provide emergency medical aid to the general public on behalf of OSY; in these situations, Agents should help by expeditiously facilitating appropriate medical care. However, Agents will render or otherwise facilitate emergency medical aid as an OSY employee, consistent with their level of successfully completed OSY sanctioned training, to any person who is:

1. An OSY protectee; or

2. In need of emergency medical aid due to the Agent's official actions.

E. **Reporting.** Agents, supervisors and/or managers must report the following to the SAPM in order to meet legal requirements, administrative needs, and interagency protocols.

1. Immediately. Agents are required to directly report to the SAPM their involvement in any of the following actions immediately, but no later than 30 minutes from the time of occurrence:

   a. Use of force that results in injury, including deadly force.

   b. Discharge of a weapon, other than during training or a use of force incident.

   c. Any frisk that discovers a weapon, regardless of whether or not the person frisked is charged with a violation of federal law.

   d. Any investigative detention or arrest of a foreign national; and any claim of diplomatic immunity by a foreign national subject to search or seizure by an Agent.

   e. Any warrantless search conducted under exigent circumstances.

   f. Any intention to arrest a juvenile or member of congress.

   g. With respect to initial appearances, whenever presentation of an arrestee will not occur for more than 4 hours, and prior to presenting an arrestee before an authorized official other than a US magistrate or district court judge.

   h. Any conflict with or concern regarding the Chief of Mission or Deputy Chief of Mission involving OSY law enforcement activities while travelling on official business for the Department.

   i. Observed human rights abuses by officers of a foreign government in a foreign country.

   j. Taking emergency action outside of OSY law enforcement authority to protect life, whether in the US or in a foreign country.

2. Within 24 hours. Managers (or their supervisors) are required to provide to the SAPM within 24 hours of occurrence:

   a. Completed USM-3A Forms (or equivalent) for Agent candidates.

   b. Notification regarding any Agent who fails to meet any requirement in Sections V, VI or VII of this Directive for continued service, fitness for duty, or the ability to execute law enforcement functions.

   c. Use of force (other than issuing simple commands that result in compliance) that does not result in injury.

   d. Notification of all searches and seizures executed under law enforcement authority.

   e. Facilitating or providing emergency medical care.

   f. Requests for other law enforcement agencies to take investigative or enforcement action on the Agent's behalf (not including routine activities within the Division's area of responsibility which do not focus on a specific person).

   g. Denial of boarding by armed Agents by an airline or government official.

h. Any intention to conduct law enforcement activities (other than executive protection assignments), obtain evidence, or propose mutual legal assistance in a foreign country; to interview or conduct a search of the person or property of a US citizen or resident alien in a foreign country; or to assist officers of a foreign government who are effecting an arrest in a foreign country.

i. Theft, loss or damage of an OSY issued weapon.

j. Notification of an Agent being named in a constitutional or state tort.

k. Division-specific guidelines or changes to existing Division guidelines applicable to Agents or OSY law enforcement functions.

X. **Promulgation.** All OSY employees appointed as Special Agents or using the "Department of Commerce Special Agent" title, credential, badge or emblem are responsible for knowing, understanding, and complying with applicable provisions of this Directive.

A. **Integration and Exceptions.** This Directive is subordinate to applicable federal laws and regulations, federal court decisions, Department Orders, and the applicable policies of government agencies with respect to delegations of law enforcement authority. Consistent therewith, the Director may grant documented exceptions to this Directive based upon the needs of OSY.

B. **Currency and Changes.** This Directive supersedes previous OSY guidance regarding Agent status, special deputation and law enforcement activities, and may only be changed or amended with the Director's written permission after review by the Office of General Counsel and SAPM. The SAPM will review this Directive on an as needed basis but not less than annually in order to ensure currency.

C. **Effects.** This Directive only provides internal OSY guidance and is not intended to, does not, and may not be relied on to create any rights, substantive or procedural, enforceable at law by any party in any matter civil or criminal. Also, this Directive does not establish limitations on otherwise lawful actions that Agents may undertake.

D. **Division-Specific Policies and Procedures.** ITMD and ESPD will establish written guidelines (subordinate to but with the same force and effect as an Appendix to this Directive) that further define specific duties for their Division activities. Written guidelines must be consistent with this Directive, and any verbal orders must be consistent with this Directive and a Division's written guidelines.

E. **Noncompliance.** Noncompliance with this Directive may form the basis for temporary suspension or permanent revocation of Agent status, potential disciplinary action up to and including termination from employment, or possible administrative sanctions, civil action, or criminal charges. Agents who are aware of guidance provided by OSY managers or supervisors that conflicts with this Directive will directly report such instances to the SAPM.

Attach #4
Resp Q7

RISK AWARENESS COMMITTEE

Purpose:

A Risk Awareness Committee is established and maintained to:

1) Ensure key Department officials who have visibility on cross-cutting functions and activities are aware of threats to Department interests
2) Accurately and regularly assess the risk of such threats to promote effective internal prioritization
3) Coordinate comprehensive Department-wide mitigation initiatives for high risk matters, without compromising investigations and/or operations
4) Implement, at the Department level, comprehensive whole-of-government responses to threats as necessary or prudent

Background:

The Office of Security's Investigations and Threat Management Division (ITMD) is responsible for identifying and investigating threats to the Department's economic advancement mission. ITMD employs a threat-based framework to objectively initiate, assess, and prioritize investigative activities. While the facts of any particular investigation articulate its threat level, information relevant to risk may reach beyond a single investigation's scope. Moreover, when a high risk exists mitigation initiatives should be implemented concurrent to but not unduly interfering with investigative activities.

Composition:

The Committee consists of the:

1) Chief Financial Officer and Assistant Secretary for Administration
2) Deputy Assistant Secretary for Administration
3) Assistant General Counsel for Administration and Transactions or Assistant General Counsel for Employment, Litigation, and Information
4) Director or Deputy Director, Office of Security
5) Special Agent in Charge or Deputy Special Agent in Charge, ITMD

All Committee members must hold an active Top Secret-SCI security clearance. Since the Committee will not receive detailed case briefings, for the inaugural meeting members may hold a Top Secret clearance while SCI is being requested.

Membership requires consenting to a non-disclosure agreement.

Re-delegation of membership or duties is not allowed.

Frequency:

The Committee will meet monthly for 1 hour, and at minimum must include Members 1, 2, 3 and 5. If a monthly meeting cannot occur, the next meeting will be scheduled within the first two weeks of the following month.

Parameters:

For each Tier I-IV open-active investigation, the Special Agent in Charge will brief the minimum amount of known information that is required to apply the Department's risk framework, identify cross-cutting functions or activities, and determine viable risk mitigation initiatives. For planning purposes, the Special Agent in Charge will also summarize Category A or B inquiries, as well as quantitative case inventory.

The following types of information will not be briefed to the Committee:

1) Information which could compromise the objectivity or integrity of an investigation
2) Information designated under law or regulation as only accessible by or available to law enforcement officers
3) Information obtained through legal process that has not been publicly released
4) Matters accepted by the US Department of Justice or a US Attorney's Office
5) Matters occurring before a grand jury
6) Matters sealed by a US court
7) Third party information designated as originator-controlled and/or limited distribution with name-only release restrictions
8) Classified information that is code word or sub-compartmented

Members may not discuss Committee briefs at any time other than during the scheduled meeting.

Outcomes:

Prior to adjourning each monthly meeting, the Committee will:

1) Evaluate risk for each open-active investigation presented
2) Identify internal actions necessary or prudent to mitigate risk without compromising investigations and/or operations addressing threat
3) Identify Departmental actions, if any, complimentary to whole-of-government responses to threats

Committee risk determinations will supersede and replace ITMD risk scoring, unless new information arises which prompts re-evaluation before a Committee meeting. Actions identified by the Committee will be incorporated as appropriate into ITMD threat management activities.

The Committee may involve other Department personnel for professional assistance on a limited basis as required by a specific investigation's circumstances, consistent with Department policy and when such involvement would not impede an investigation or operation.

ITMD staff will memorialize and retain all Committee decisions.

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

February 19, 2019

MEMORANDUM FOR SECRETARY ROSS

FROM: Peggy E. Gustafson
Inspector General

SUBJECT: Follow-up Request for Information Pursuant to the Inspector General Act of 1978, as Amended

This request for information supplements the initial request provided to you on November 19, 2018 concerning the mission, authority, and activities of the Investigations and Threat Management Division (ITMD). The Office of Inspector General (OIG) has reviewed the Department's December 20, 2018 response (the Response) as well as the associated documents and has some follow-up questions. The OIG requests that you provide responses to the following questions, with relevant documents, by March 5, 2019.

Questions Related to ITMD's Possible Counterintelligence Role

The Response to Question 2 of the November 19 request states that ITMD carries out its mission by conducting investigations and operations to protect against mission-critical threats and that such activities may involve administrative or law enforcement techniques. One of the documents referenced within Attachment 3 to the Response, the *ITMD Inquiry and Investigation Guide* from April 2014, contains a page outlining "baseline steps" for performing "Counterintelligence Inquiries." *Id.* at 10. Further, Department Administrative Order (DAO) 207-1 states that ITMD conducts "counterintelligence investigations involving personnel (e.g., foreign national visitors)." Given that the Response omits discussion of any counterintelligence function, the OIG has the following questions.

1. Does ITMD perform "counterintelligence inquiries" or "counterintelligence investigations"? If so, please define or describe each function, as applicable.

2. Please describe the scope of "counterintelligence inquiries" or "counterintelligence investigations."

3. Please describe any other counterintelligence role or function performed by ITMD not described above.

4. Please explain the legal authority, statutory, regulatory, or otherwise, under which ITMD undertakes the activities described within your responses to the first and third items above. Please explicitly associate the authority to the functions.

5. Please provide a list of the training and certifications that ITMD personnel receive to enable them to conduct activities described within your responses described above.

6. The supplemental letter in support of deputation (Attachment 1 to the December 20, 2018 response) appears to support deputation for protection of the Secretary and Department critical assets. DAO 207-11, Official Credential and Badge, notes that special agents within OSY may be "deputized for mission-critical threat and counter-intelligence functions." Are any ITMD agents deputized for "counter-intelligence functions"? If so, under what authority have such deputations been executed?

7. In reply to the seventh question of the November 19 request regarding oversight of ITMD, the Response indicates that ITMD was reviewed by the National Counterintelligence and Security Center in 2011, 2013, and 2016. Please describe these reviews. Please also answer the following:

    a. Please confirm that the National Counterintelligence and Security Center is under the Office of the Director of National Intelligence (ODNI).
    b. According to the National Counterintelligence and Security Center's publicly available information, it came into existence in 2014. In light of this, please indicate what entity conducted the aforementioned reviews in 2011 and 2013.
    c. Were such reviews conducted of the Department's counterintelligence or security activities?

8. Did the reviews by ODNI referenced in the above question involve determining whether ITMD has authority to conduct any counterintelligence inquiry, investigation, or function? If so, please share the findings with the OIG in response to this request.

9. Since July 2017, has the Department sought clarification from ODNI or any of its components on ITMD's authority to carry out any counterintelligence inquiry, investigation, or function? If so, please share ODNI's response with the OIG in response to this request.

10. If ITMD does not conduct counterintelligence inquiries, investigations, or functions, are counterintelligence matters referred to other agencies? If so, please generally describe the referral process, including what occurs when an agency declines such referrals.

Questions Related to the Federal Senior Intelligence Coordinator Role

In reply to the first question of the November 19 request regarding the mission of ITMD, the Reply states that ITMD currently serves as the Department's Federal Senior Intelligence Coordinator pursuant to a 2017 designation by the Deputy Secretary. The OIG has the following questions regarding this designation and role.

11. We understand that the Office of Executive Support previously served as the Department's Federal Senior Intelligence Coordinator. Is that correct?

    a. Please indicate when the Office of Executive Support stopped fulfilling this function.

12. Please describe ITMD's role as the Federal Senior Intelligence Coordinator.

13. Please explain the legal authority, statutory, regulatory, or otherwise, such as a legal agreement, under which ITMD performs the role of the Federal Senior Intelligence Coordinator.

14. Please provide a list of the training and certifications ITMD personnel receive to enable them to conduct any activities described within your responses to the twelfth question.

15. What Department Organization Order (DOO) and DAO prescribe the functions and responsibilities of the Federal Senior Intelligence Coordinator?

In addition, the OIG asks that you produce any additional documentation or information deemed relevant to this request for information. If there is no such documentation, please state so. The OIG asks for answers to the above questions through an unclassified response.

The Inspector General Act of 1978 guarantees the OIG timely access to "all records, reports, audits, reviews, documents, papers, recommendations or other materials" available to the Department,[1] and authorizes the IG to "make such investigations and reports relating to the administration of programs and operations of [the Department] as are, in the judgment of the Inspector General, necessary or desirable[.]"[2] DAO 213-2, § 4.03 states that "it is Department policy that all employees fully cooperate with the OIG," and that "Departmental officials shall make every effort to assist the OIG in achieving the objective of effective inspections and evaluations." Similarly, DOO 10-13, § 4.01 states that "[t]he officers and employees of the Department shall cooperate fully with the officials and employees of the OIG and shall provide such information, assistance, and support without delay as is needed for the OIG to properly carry out the provisions of the [Inspector General] Act [of 1978]."

If you have any questions or need additional information, please contact me at (202) 482-4661.

---

[1] 5 U.S.C. App. § 6(a)(1)(A).
[2] *Id.* § 6(a)(2).

UNITED STATES DEPARTMENT OF COMMERCE
Chief Financial Officer and
Assistant Secretary for Administration
Washington, D.C. 20230

MAY 2 1 2019

MEMORANDUM FOR THE INSPECTOR GENERAL

FROM: Richard L. Townsend
Director for Security

SUBJECT: Follow-up Response to Request for Information Pursuant to the Inspector General Act of 1978, as Amended

This memorandum serves to transmit materials responsive to your follow-up request for information provided to Secretary Ross on February 19, 2018 seeking additional information related to the Office of Security's Investigations and Threat Management Division.

Attached you will find responses to the enumerated questions; however, portions of the requested materials and context associated with them are best provided via a classified briefing in a controlled environment attended by those holding appropriate clearance levels.

If you have any questions or should you or a member of your staff require a classified briefing, please contact me at (202) 482-4371 or rtownsend@doc.gov.

ATTACHMENT

1. Follow-up Response to Request for Information Pursuant to the Inspector General Act of 1978, as Amended

After reviewing the *Follow-up Request for Information Pursuant to the Inspector General Act of 1978, as Amended* dated February 19, 2019, we can now provide greater context about ITMD's use of the term "counterintelligence". Although ITMD does not operate a dedicated counterintelligence program, does not originate investigative activities solely with the intent of engaging in counterintelligence, and does not engage unilaterally in traditional US Intelligence Community (USIC) counterintelligence operations, it does act broadly to protect the Department's critical assets. While certain threats identified and investigated by ITMD may also be characterized as counterintelligence concerns, ITMD does not engage such concerns without a corresponding civil or criminal law enforcement responsibility. We reiterate that at all times, regardless of the use of the phrase "counterintelligence inquiry," "counterintelligence investigation," or "counterintelligence program" in any documentation, all ITMD operations are in support of our core mission to protect Department critical assets.

The current *National Counterintelligence Strategy of the United States* asserts that "countering FIE (Foreign Intelligence Entity) threats is a core obligation across the US Government [and that we must] widen counterintelligence practices across the US Government." In support of this Strategy, the National Counterintelligence and Security Center (NCSC) advocates for Federal Partners – which includes Commerce – to implement counterintelligence and security programs not funded by the National Intelligence Program. NCSC also acknowledges the different missions and authorities of various US Government departments and agencies.

We hope the responses below satisfy your review. Please let us know if you require additional information.

Questions Related to ITMD's Possible Counterintelligence Role

1. Does ITMD perform "counterintelligence inquiries" or "counterintelligence investigations"? If so, please define or describe each function, as applicable.

Protecting against threats is a core function of the security discipline, and ITMD is specifically chartered to protect against mission-critical threats to the Department. To this end, ITMD conducts investigative activities to identify and protect against threats to Commerce assets; as such, these investigative activities may involve threats posed by FIEs. Although ITMD does not operate a dedicated counterintelligence program, some mission-critical threats posed against the Department may also be characterized as counterintelligence concerns. Thus, ITMD's investigative activities may lead to the discovery of threats that can be both a national security and criminal concern.[1]

[1] In our December 20, 2018 response to Question 6 of OIG's request, we answered "ITMD casework involves strategic or tactical level threats to the Department's critical assets, which can be of a national security and/or criminal nature". For example, the final Report of Investigation for 2015089 categorized this particular case as "Criminal/Counterintelligence"; while the criminal conduct documented an individual's culpability under law, it also represented a larger (and criminally uncodified) strategic counterintelligence threat to the greater national

Executive Order (EO) 12333 (as amended) defines counterintelligence, in relevant part, as: "information gathered and activities conducted to identify [...] or protect against [...] intelligence activities [...] conducted for or on behalf of foreign powers, organizations, or persons, or their agents". ITMD does not engage in foreign intelligence or counterintelligence activities as proscribed by EO 12333,[2] but instead acts to protect against mission-critical threats to the Department.[3] Specifically, the *National Counterintelligence Strategy of the United States* directs departments and agencies – not only USIC members – to safeguard assets from FIEs, as well as build and strengthen programs to counter their efforts. Furthermore, NCSC's *Countering Foreign Intelligence Threats: Implementation and Best Practices Guide* recommends that departments and agencies establish a formal organizational construct for countering FIE threats.

ITMD processes all investigative matters aimed at preventing threats to Department critical assets (including those which may involve FIE threats) through intake, inquiry, and/or investigation phases (matters lacking a suspicion or allegation but received by the office are deemed intake; matters having a suspicion/allegation are deemed inquiries subject to authentication; and matters with an authenticated suspicion/allegation are deemed investigations subject to a finding that the suspicion/allegation is substantiated or unsubstantiated).

2. Please describe the scope of "counterintelligence inquiries" or "counterintelligence investigations."

With respect to the scope of any ITMD inquiry process (including those which may involve FIE threats), in order to authenticate a suspicion or allegation so that additional resources are allocated, ITMD special agents use investigative techniques permitted by their administrative and law enforcement authorities to develop evidence that demonstrates the basis for investigation is founded (and is not fictitious, baseless or improper), meets mission requirements (including threat actor interest, whether a potential threat or inchoate criminal violation exists, and if there is an opportunity to prevent or mitigate the threat), and is solvable (if additional leads can be developed to answer the question posed by the investigative basis). The *2014 ITMD Guide* included a section specific for inquiries which may represent FIE threats to assist special agents with researching and identifying information and circumstances which

---

security of the United States. After ITMD identified this threat, OIG was directly consulted, participated in this investigation, and later described this case in its *March 2018 Semiannual Report to Congress*.

[2] In our December 20, 2018 response to Question 5 of OIG's request, we informed you the Department was not a member of the USIC.

[3] When ITMD exercises its law enforcement authority to protect against mission-critical threats to the Department – including FIE threats that involve what may be characterized as counterintelligence concerns – our reading of EO 12333 is that it does not "apply to or interfere with any authorized civil or criminal law enforcement responsibility of any department or agency". Conversely, EO 12333 specifies USIC members are authorized to "participate in law enforcement activities to investigate or prevent clandestine intelligence activities by foreign powers".

may bear on these three constructs (foundation, mission, and solvability); developed material may also carry over into the next phase of investigation as well.

With respect to the scope of any ITMD investigation process (including those which may involve FIE threats), threats may not necessarily align to a statutory violation but nonetheless must be identified, assessed and managed. In order to determine whether the basis for investigation is substantiated or unsubstantiated, ITMD special agents use investigative techniques permitted by their administrative and law enforcement authorities to discern threat by developing evidence that demonstrates the value of a Department asset or activity to an adversary, the nexus of the adversary to the asset/activity, and adversarial action in relation to compromising the asset/activity; while working through this construct, agents concurrently develop any evidence of statutory violations.

3. Please describe any other counterintelligence role or function performed by ITMD not described above.

Our answers to Questions 1 and 2 focus on investigative activities. Additionally, pursuant to Department policy ITMD is the executing program office for Commerce's Insider Threat Program, which involves identifying through analysis and investigation insider threats that may also be characterized as counterintelligence concerns. As a by-product of its investigative mission ITMD also conducts classified and unclassified research, internal and external liaison, and Division-produced analysis to enhance identification, assessment, and awareness of mission-critical threats, which may also include counterintelligence concerns.

Furthermore, since a primary purpose of ITMD is to prevent or mitigate mission-critical threats, when warranted ITMD takes threat management actions based on evidence that a high threat – including those which may also be characterized as counterintelligence concerns – is adversely impacting the Department. These actions involve protecting the Department's critical assets and activities by countering adversarial efforts to exploit or compromise them.[4]

Finally, ITMD serves as a principal representative of the Department with National Security Staff for national strategies and policy that addresses mission-critical threats (including those which may also involve counterintelligence).

4. Please explain the legal authority, statutory, regulatory, or otherwise, under which ITMD undertakes the activities described within your responses to the first and third items above. Please explicitly associate the authority to the functions.

[4] Threat management actions are coordinated internally (for example, removing a specific entity from access to critical assets/activities, or informing the Risk Awareness Committee of a systemic concern), or externally with key US Government stakeholders (for example, providing ITMD investigative findings to decision-makers for US Government strategic policy initiatives, or otherwise collaborating with other law enforcement or USIC partners).

All ITMD investigative and threat management activities – including mission-critical threats posed against the Department that may also be characterized as FIE threats – are conducted under the Division's administrative and law enforcement authorities described in Questions 3 and 6 of our December 20, 2018 response. Specifically, for threats without a corresponding criminal violation, ITMD exercises the administrative authorities described in Chapter 36 of the Department's Manual of Security Policies and Procedures. For threats with a corresponding potential criminal violation, ITMD protects the Department's critical assets under its USMS special deputation for critical assets or 40 U.S.C. § 1315 authority. For either type of threat, ITMD may also exercise authorities vested in the Secretary in order to perform certain functions and responsibilities assigned to the Office of Security pursuant to DOO 20-6, Section 4. ITMD does not engage unilaterally in traditional USIC counterintelligence operations; where ITMD lacks specific authority, it acts in conjunction with other law enforcement or USIC partners, and these activities are conducted, with Commerce management approval, under the request or approval and authorities of the respective partner agency and not the Department. In the past, ITMD has also received special deputations applied for by and issued to partner agencies that were unique to specific task force assignments.

ITMD's insider threat role includes the above authorities as applicable under the ambit of Executive Order 13587 and implementing guidelines, and the Department's separate implementation policy. The Division's authority to perform research, liaison and analysis, and represent the Department with National Security Staff is contained in Chapter 36 of the Department's Manual of Security Policies and Procedures.

5. Please provide a list of the training and certifications that ITMD personnel receive to enable them to conduct activities described within your responses above.

In the above responses, we have described ITMD activities necessary to accomplish the Division's mission to protect Department critical assets. Pursuant to special deputation and 40 U.S.C. § 1315 requirements, Office of Personnel Management (OPM) series 1811 (criminal investigator) personnel are graduates of a basic law enforcement training program, and OPM series 0132 (intelligence specialist) personnel are graduates of a basic intelligence analysis training program; personnel receive additional law enforcement and/or intelligence training, as well as internal ITMD training for mission, authority, and protocols/processes. Due to the Department's unique role in economic and national security, internal awareness training is specifically provided to ITMD staff for mission-critical threats (including FIE threats).[5]

In order to better execute its core mission to protect the Department's critical assets, ITMD may select applicants who have already received specific training in FIE efforts and

[5] ITMD has also provided awareness and investigative briefings regarding emerging strategic threats to US economic advancement to other internal (including Inspector General Gustafson) and external entities (including National Security Staff, Central Intelligence Agency, Federal Bureau of Investigation, Department of Defense, and key portions of the USIC and Federal law enforcement communities).

counterintelligence matters, in addition to sending on-board staff to training. Currently, the Division has staff who have completed the following courses:

- Counterintelligence Managers Seminar, Joint Counterintelligence Training Academy
- Strategic Approaches to Counterintelligence, Federal Bureau of Investigation
- National Security Policy and Counterintelligence Implications of Denial and Deception Practices, Central Intelligence Agency
- Security Asset Protection Professional Certification, Department of Defense
- Insider Threat Hub Operations Course, National Insider Threat Task Force
- Counterintelligence Fundamentals, Central Intelligence Agency
- Overview of Critical Counterintelligence Issues, Central Intelligence Agency
- Counterintelligence Force Protection, Joint Counterintelligence Training Academy
- Counterintelligence Case Studies, Department of Energy
- Offensive Counterintelligence Operations, Central Intelligence Agency
- Counterespionage, Central Intelligence Agency
- Cyber Counterintelligence, Joint Counterintelligence Training Academy
- Human Asset Validation, Central Intelligence Agency
- Cultural Considerations in Counterintelligence Interviewing and Elicitation, Joint Counterintelligence Training Academy
- National Collaboration Course, National Collaboration Development Center
- Countersurveillance, Joint Counterintelligence Training Academy
- Multiple country-specific counterintelligence seminars, Central Intelligence Agency and Joint Counterintelligence Training Academy

ITMD also screens applicants and has employed staff with foreign language and other capabilities that align with mission-critical threat concerns.

After its 2014 review of the Department's Insider Threat program, NCSC's National Insider Threat Task Force states, in relevant part:

> The Insider Threat program employs an experienced program manager with law enforcement, security, investigative, and counterintelligence expertise, and is staffed with program personnel who are trained and skilled in law enforcement, counterintelligence and security fundamentals [...]

6. The supplemental letter in support of deputation (Attachment 1 to the December 20, 2018 response) appears to support deputation for protection of the Secretary and Departmental critical assets. DAO 207-11, Official Credential and Badge, notes that special agents within OSY may be "deputized for mission-critical threat and counter-intelligence functions." Are any ITMD agents deputized for "counter-intelligence functions"? If so, under what authority have such deputations been executed?

Prior to your request, we were actively working with the Office of General Counsel and Office of Privacy and Open Government to remove the reference to "counter-intelligence" in DAO 207-11. This language was added by Thomas Predmore during his tenure as Director for Security. On its face it is a description of functions, and not the specific terms of deputation (to protect the Department's critical assets) which were provided with our December 20, 2018 response. The Department will more specifically describe ITMD's authority in a revision of DAO 207-11 to reflect our draft Special Agent Directive, which we previously submitted to the OIG.

7. In reply to the seventh question of the November 19 request regarding oversight of ITMD, the Response indicates that ITMD was reviewed by the National Counterintelligence and Security Center in 2011, 2013, and 2016. Please describe these reviews.

NCSC noted that the Department is not a USIC member, but conducted a discretionary review in 2011 as the US Government's first non-USIC member "due to its established background and good relations with IC members." In addition to the 2011 review, NCSC conducted a 2013 review; both were in a classified setting at their headquarters. The 2011 review included a presentation and discussion of ITMD's mission, authorities and significant investigative casework, followed by questions posed by a leadership team panel (including the National Counterintelligence Executive and his Deputy, as well as detailees from other government agencies); the 2013 review was similar, but conducted by a smaller panel. The 2016 review required answering a series of written interrogatories at a classified level.

Please also answer the following:

7a. Please confirm that the National Counterintelligence and Security Center is under the Office of the Director of National Intelligence (ODNI).

The NCSC website indicates that NCSC is a component of ODNI.[6]

7b. According to the National Counterintelligence and Security Center's publicly available information, it came into existence in 2014. In light of this, please indicate what entity conducted the aforementioned reviews in 2011 and 2013.

The 2011 and 2013 reviews were conducted by the Office of the National Counterintelligence Executive. According to their website, NCSC was preceded by the Office of the National Counterintelligence Executive; the National Counterintelligence Executive also serves as the NCSC Director.

7c. Were such reviews conducted of the Department's counterintelligence or security activities?

[6] https://www.dni.gov/index.php/ncsc-home

The 2011, 2013 and 2016 Mission Reviews were conducted on the Department's activities that involved FIE threats. Below is an excerpt from the 2011 review. We note this review refers to the "Commerce CI program", but as stated above ITMD executes an overall mission-critical threat function (which was explained during these reviews) that can include FIE threats which may also be characterized as counterintelligence concerns:

> My staff and I have recently concluded [...] Mission Reviews, a process that included a review of the Department of Commerce CI program. This is the first time we have reviewed the counterintelligence program of a department or agency not in the Intelligence Community (IC) [...] Moreover, there are several critical assets found in your Department that may be of interest to foreign intelligence services (FIS) and your CI program's efforts in protecting those assets is crucial to U.S. national security. I am confident that with sufficient resources [...] the Commerce CI program will continue to develop into a model program for other non-IC departments and agencies in the US Government.

8. Did the reviews by ODNI referenced in the above question involve determining whether ITMD has authority to conduct any counterintelligence inquiry, investigation, or function? If so, please share the findings with the OIG in response to this request.

Please see our answers for Questions 7 and 7c, above. At no time has the Department been notified by the NCSC Director (who according to their website is ODNI's National Intelligence Manager for Counterintelligence, and since 2010 has been an official from the Federal Bureau of Investigation) that despite comprehensive reviews, the Department has acted without authority or otherwise improperly.

Below is an excerpt from the 2011 review that cites ITMD's overarching proactive investigative methodology as applied to FIE threats:

> Commerce's CI proactive investigative methodology [and an associated CI analytical construct] are excellent initiatives and have potential applications elsewhere in the CI community. These capabilities have proven effective in identifying and mitigating threats with minimal resource impact and they develop information of potential interest to other elements in the CI community.

Use of agency-specific authorities to protect against FIE threats to critical assets has prominently figured in Federal doctrine for some time and continues to be reflected in the current *National Counterintelligence Strategy of the United States*. The 2013 review states in relevant part:

> The results of this review reinforce my belief that the state of national CI continues to improve and that the efforts of the Commerce Department's Office of Security, and especially the Investigations and Intelligence Division [ITMD], are of great value. Nevertheless, significant challenges remain. As a community, we must use all available

authorities and capabilities to counter the activities of FIS targeting our critical assets [...] A proactive and well-resourced CI program, working in tandem with an equally effective security program, is essential to counter [FIS] efforts and protect both the vital classified and unclassified programs in the Department of Commerce [...] The Department of Commerce's CI and security efforts are strong and a successful model for other agencies.

9. Since July 2017, has the Department sought clarification from ODNI or any of its components on ITMD's authority to carry out any counterintelligence inquiry, investigation, or function? If so, please share ODNI's response with the OIG in response to this request.

No. We are unaware of any need to seek clarification for ITMD's authority to carry out any inquiry, investigation, or function that involves protecting against FIE efforts which may also be characterized as counterintelligence, inasmuch as these actions are within the ambit of ITMD's mission and our answers in this and our prior response to the OIG. NCSC's current Strategic Plan specifically cites the Department of Commerce as a stakeholder linked to NCSC by governance, oversight and resources, and advocates for Federal Partners to implement "CI and security programs not funded by the National Intelligence Program". If the OIG is aware of a specific circumstance since July 2017 that requires clarification, please advise and we will provide an additional response.

10. If ITMD does not conduct counterintelligence inquiries, investigations, or functions, are counterintelligence matters referred to other agencies? If so, please generally describe the referral process, including what occurs when an agency declines such referrals.

Please see our answers to Questions 1 and 3. Moreover, ITMD routinely receives referrals for FIE threats that may also be characterized as counterintelligence concerns from other Federal law enforcement and USIC entities (including the Federal Bureau of Investigation and the Central Intelligence Agency) and informs other entities of ITMD-identified threats as necessary (including the OIG). Additionally, when a law, regulation or policy requires a referral from ITMD to another entity, we provide proper notification and execute such referrals; these referrals can sometimes result in joint casework or investigative assistance between the receiving entity and ITMD.

<u>Questions Related to the Federal Senior Intelligence Coordinator Role</u>

11. We understand that the Office of Executive Support previously served as the Department's Federal Senior Intelligence Coordinator. Is that correct?

Yes.

11a. Please indicate when the Office of Executive Support stopped fulfilling this function.

It is our understanding that the Director, Office of Executive Support served as the Department's Federal Senior Intelligence Coordinator (FSIC) until June 2016.

12. Please describe ITMD's role as the Federal Senior Intelligence Coordinator.

Pursuant to Intelligence Community Directive (ICD) 404, the FSIC is the primary liaison between the Department and the USIC. According to the FSIC Handbook, FSICs "are the central locus of intelligence concerns for their agencies".

[redacted] and [redacted] were designated with the FSIC role on June 1, 2017 by Ellen Herbst, performing the non-exclusive duties of the Deputy Secretary of Commerce. The FSIC role was designated to ITMD personnel due to a continuing need by the Department and USIC in the functional absence of the Office of Executive Support.

In accordance with the FSIC Handbook and ITMD's mission and casework, the Division's role has been to coordinate and facilitate intelligence requirements, support and expertise; understand counterintelligence threats to the Department; oversee the Department's Insider Threat program; and protect Department facilities and data.

13. Please explain the legal authority, statutory, regulatory, or otherwise, such as a legal agreement, under which ITMD performs the role of the Federal Senior Intelligence Coordinator.

The FSIC role is an internal designation made by the Department.

14. Please provide a list of the training and certifications that ITMD personnel receive to enable them to conduct any activities described within your responses to the twelfth question.

ICD 404 does not require specific training or certification as eligibility for FSIC designation. FSICs can make training needs known to ODNI, which acknowledges these needs will vary due to size and experience level of departments and agencies. ITMD staff already possess training in the FSIC areas described in Question 12. Additionally, current ITMD staff are graduates of the following programs:

- Senior Executives in National and International Security, Kennedy School of Government
- National Senior Intelligence Course, Joint Military Intelligence Training Academy
- Special Operations Intelligence Leaders Course, US Special Operations Command
- USIC Operations and Analysis Course, Central Intelligence Agency
- Intelligence Analysis Training Program, Federal Law Enforcement Training Center

15. What Department Organization Order (DOO) and DAO prescribe the functions and responsibilities of the Federal Senior Intelligence Coordinator?

Since issuance of ICD 404, we are unaware of any DOO or DAO that has specifically included a FSIC. Currently, the Department is drafting a suitable memorialization of this role.

Twenty-five (25) Pages Withheld In Full Pursuant to (B)(7)(A)

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

June 7, 2019

MEMORANDUM FOR SECRETARY ROSS

FROM: Peggy E. Gustafson
Inspector General

SUBJECT: Reply to May 21, 2019 Response to Follow-up Request for Information Pursuant to the Inspector General Act of 1978, as Amended

The Office of Inspector General (OIG) sent a request for information to you on November 19, 2018 concerning the mission, authority, and activities of the Investigations and Threat Management Division (ITMD). After reviewing the Department's December 20, 2018 response and associated documents, the OIG had several follow-up questions attempting to clarify ITMD's potential role in counterintelligence activities. In a memorandum dated February 19, 2019, the OIG requested that the Department provide responses to the follow-up questions, with relevant documents, by March 5, 2019. Despite several attempts by the OIG, the Department's response to these follow-up questions was not received until May 21, 2019.

As an initial matter, there is concern about the length of time taken to respond to fundamental questions about ITMD's mission and organic legal authority. However, the OIG has reviewed the May 21, 2019 response and found it generally useful in clarifying the role of ITMD with regard to several public mission statements and internal descriptions using the word "counterintelligence." The OIG now understands from the Department's response that ITMD does not operate a dedicated counterintelligence program, does not originate investigative activities solely with the intent of engaging in counterintelligence, and does not engage unilaterally in traditional U.S. Intelligence Community counterintelligence operations.

In order for the OIG to close this matter out, consistent with the Department's May 21, 2019 response, the OIG requests that you respond to the following, with the relevant documents, by June 21, 2019:

1. The OIG noted that Department Administrative Order (DAO) 207-11, Official Credential and Badge, states that special agents within the Office of

Security may be "deputized for mission-critical threat and counter-intelligence functions." The Department has responded that it is actively working to remove the "counter-intelligence" reference from the DAO given that it is not a specific term of deputation, and will more specifically describe ITMD's authority in a revision of DAO 207-11. Please provide the revised draft DAO to the OIG.

2. Similarly, DAO 207-1 states that ITMD conducts "counterintelligence investigations involving personnel (e.g., foreign national visitors)." If the Department believes this wording could be made more accurate, as with DAO 207-11, please let the OIG know the process and timeline for any revision.

3. In response to a question about the *ITMD Inquiry and Investigation Guide* from April 2014 containing a page outlining "baseline steps" for performing "Counterintelligence Inquiries," the Department explained that the inquiries involve potential Foreign Intelligence Entity threats to Department assets. If the Department believes the header description to these inquiries could be made more accurate, please let the OIG know the process and timeline for any revision.

4. The Department stated that since the issuance of Intelligence Community Directive 404, the Department is unaware of any Department Organization Order (DOO) or DAO that specifically includes a Federal Senior Intelligence Coordinator and that the Department is drafting a memorialization of the role. Please provide such memorialization, whether in DOO, DAO, or otherwise, to the OIG.

As a reminder, the Inspector General Act of 1978 guarantees the OIG *timely* access to "all records, reports, audits, reviews, documents, papers, recommendations or other materials" available to the Department[1] and authorizes the Inspector General to "make such investigations and reports relating to the administration of programs and operations of [the Department] as are, in the judgment of the Inspector General, necessary or desirable[.]"[2] DAO 213-2, § 4.03 states that "[i]t is Department policy that all employees fully cooperate with the OIG," and that "Departmental officials shall make every effort to assist the OIG in achieving the objective of effective inspections and evaluations." Similarly, DOO 10-13, § 4.01

[1] 5 U.S.C. App. § 6(a)(1)(A).
[2] *Id.* § 6(a)(2).

states that "[t]he officers and employees of the Department shall cooperate fully with the officials and employees of the OIG and shall provide such information, assistance, and support without delay as is needed for the OIG to properly carry out the provisions of the [Inspector General] Act [of 1978]."

If you have any questions or need additional information, please contact me at (202) 482-4661.

UNITED STATES DEPARTMENT OF COMMERCE
Chief Financial Officer
Assistant Secretary for Administration
Washington, D.C. 20230

JUN 14 2019

MEMORANDUM FOR THE INSPECTOR GENERAL

FROM: Richard L. Townsend
Director for Security

SUBJECT: Follow-up Response to Request for Information Pursuant to the Inspector General Act of 1978, as Amended

This memorandum serves to transmit materials responsive to your follow-up request for information provided to Secretary Ross on June 7, 2019 seeking additional information related to the Office of Security's Investigations and Threat Management Division.

Attached you will find responses to the enumerated questions. If you have any questions or should you or a member of your staff require a classified briefing, please contact me at (202) 482-4371 or rtownsend@doc.gov.

ATTACHMENT

1. Follow-up Response to Request for Information Pursuant to the Inspector General Act of 1978, as Amended

This letter contains the Department's response to the Inspector General's *Reply to May 21, 2019 Response to Follow-up Request for Information Pursuant to the Inspector General Act of 1978, as Amended,* dated June 7, 2019. Please let us know if you have any additional questions.

1. Department Administrative Order (DAO) 207-11, *Official Credential and Badge*, Section 2.03(e) will be revised to remove the phrase "counterintelligence" and will read as follows. As requested, a draft copy of the DAO is also attached. Please note that this language is not entirely concrete as a possible reorganization may alter the location of certain functions within OSY.

   > Special Agents assigned to the Investigations and Threat Management Division [or Office, or Service, depending on the reorganization] shall be issued the Form CD-277 and Special Agent Badge to perform all duties conferred upon them under the laws of the United States and the regulations of the Department, and may exercise authority vested in the Secretary or otherwise provided to the [Division, or Office, or Service], including the authority to protect the Department's critical assets and activities, investigate, bear firearms, make arrests, administer oaths, apply for and execute legal process, and require and receive information on matters regarding the laws and regulations of the United States and the Department.

2. DAO 207-1, *Security Programs*, Section 4.01(a)(6), will be revised to remove the reference to counterintelligence and will read as follows. As with the response to #1 above, please note that it is our intent to work with the Office of Privacy and Open Government to implement this change as soon as possible, however, this may take time as DAO 207-1 is connected to changes related to a possible reorganization.

   > The Investigations and Threat Management Division [or Office, or Service, depending on the reorganization], through conducting sensitive and complex national security and criminal investigations, identifies, assesses and protects against threats to the Department's assets and activities which if compromised would cause significant damage to US economic advancement, the US Government's ability to function, or Departmental functions in support of those concerns.

3. The header will be revised to state "National Security Inquiries."

4. Please find below a comprehensive response to this request, which necessitates that we provide an explanation of the history and past actions that have removed the memorialization of the Federal Senior Intelligence Coordinator role from the DOOs.

RESPONSE #4

History of the Federal Senior Intelligence Coordinator (formerly known as the Senior Intelligence Advisor and Senior Liaison/ Representative to the Intelligence Community)

On March 28, 1978 and after an agreement between Commerce and the Intelligence Community,[1] the Department of Commerce established the Office of Intelligence Liaison (OIL) by issuing a Department Organization Order (DOO) and providing official notice in the Federal Register.[2] While OIL originally reported to Assistant Secretary, OIL began reporting to Deputy Assistant Secretary for Operations when the DOO was reissued in the Federal Register, effective October 14, 1980.[3] OIL's Director served as Commerce's Senior Intelligence Advisor and Senior Liaison/ Representative to the Intelligence Community, in addition to his managerial responsibilities.

Less than a year later, in June 1981, OIL began reporting to the Office of General Counsel (OGC).[4] On March 7, 1996, Commerce officials re-designated OIL as the Office of Executive Support (OES),[5] citing "security considerations"[6] and "avoiding misapprehensions regarding the functions of the office."[7] While no changes were made to the office's mission, duties, budget, or staff,[8] OES's duties and responsibilities were no longer delineated within any Department Organizational Order (DOO).

The Office of Executive Support serves as the Department's primary liaison with the Intelligence Community (IC). Key liaison tasks include intelligence requirements management, reporting/product evaluations, and facilitating relationship building and information sharing between Commerce policy, security, scientific and technological offices and IC analysts. Generally, the OES Director is designated by the Secretary to serve as the Federal Senior Intelligence Coordinator (FSIC).[9] The FSIC is the primary liaison between the Department and the Intelligence Community, with entrusted responsibilities in the areas of intelligence, security, counterintelligence, counterterrorism, insider threat and cybersecurity.[10] The FSIC represents the Department at the Non-Title 50 (NT50) agency meetings of the FSIC Advisory Board within the Office of the Director of National Intelligence.

---

[1] Memorandum of Understanding (MOU) between Commerce and the IC, dated May 5, 1977
[2] DOO 20-15, 43 Fed. Reg. 15476 (March 28, 1978).

[3] DOO 20-15, effective October 14, 1980: 45 Fed. Reg. 75264 (Nov. 14, 1980)
[4] DOO 10-6: OGC, Effective July 9, 1981
[5] DOO 10-6: OGC, effective March 7, 1996
[6] Memorandum from General Counsel to Raymond Kammer, "Request for Redesignation of Office," dated February 27, 1996
[7] Memorandum from Chief of General Law Division to Sherry Cage, OMB, "Revision of DOO 10-6," dated June 27, 1995
[8] Form SEC-20 Clearance Sheet, Revision of DOO 10-6
[9] CFO/ASA Herbst re-designated the FSIC to the Assistant Director, Investigations and Threat Management Division, given the suspension of OES activities during OSY's investigation.

[10] FSIC Handbook, Office of the Director of National Intelligence

On June 6, 2016, OES became non-operational due to an internal investigation by the Investigations and Threat Management Division (ITMD), CFO/ASA/OSY. Due to the ongoing investigation and suspension of OES services, the previous administration's CFO/ASA performing the non-exclusive functions of the Deputy Secretary temporarily reassigned the FSIC responsibilities to ITMD, while delegating logistical functions to the Bureau of Industry and Security (BIS).

In addition to the FSIC functions performed by ITMD staff, logistical functions performed by BIS included providing a SCIF to the Office of the Secretary (OS) and OGC while the OS/OGC SCIF space remained closed by ITMD investigators, the handling of TS/SCI documents, and facilitating timely communication with the NSC. But while these stop gap measures helped to mitigate a complete intelligence void by keeping the Secretary and other key officials briefed, it did not obviate the need to fully provide, rather than only facilitate and coordinate, intelligence support services for the Department.

The CFO/ASA recognized this gap and immediately initiated a review and is now in the process of realigning the Department's FSIC responsibilities and moving the intelligence workload formerly performed by OES to report to a new Deputy Assistant Secretary for Security. This realignment includes consolidating the ITMD functions alongside this new operating unit and adding more cohesive oversight and coordination into the reporting chain between the FSIC, ITMD and OSY. Specifically, the CFO/ASA is preparing a reprogramming request to reinstate the Deputy Assistant Secretary for Security (originally created in 1998) as a position to oversee the Department's Investigations and Threat Management Division (or Office, or Service, depending on the reorganization), a re-designed intelligence office with FSIC responsibilities, and OSY. Notably, the DAS for Security is still referenced in the Code of Federal Regulations as the DOC official responsible for implementing the regulations and executive order that deal with the classification, declassification, and public availability of national security information.[11] The Department is memorializing the realignment as part of a reprogramming request and plans to incorporate these changes as part of the revision to DOO 20-6, and DAO 207-1. I assure you that we will copy you on the reprogramming request as soon as it is complete. Please do not hesitate to reach out to me directly to discuss the status of the FSIC role and our new organizational plan.

[11] 15 C.F.R. §§ 4a.2; 4.10(c).

TRANSMITTAL _____

United States of America DEPARTMENT OF COMMERCE	DEPARTMENT ADMINISTRATIVE ORDER 207-11	
DEPARTMENT ADMINISTRATIVE ORDER SERIES	DATE OF ISSUANCE	EFFECTIVE DATE

OFFICIAL CREDENTIAL AND BADGE

SECTION 1. PURPOSE.

.01 This Order prescribes: a uniform Official Credential for the Department of Commerce (the Department) law and regulatory enforcement units and offices authorized to conduct official law enforcement and non-law enforcement investigations; the official badges for use by special agents, enforcement officers, and other personnel performing law enforcement and non-law enforcement duties; and policy and procedures for the issuance and use of official credentials and badges.

.02 This revision: updates language to reflect the organizational realignment of secretarial protection functions to the Immediate Office of the Secretary thus replacing the words "Office of Security" with "Office of the Secretary" in Section 2.03d. Additionally, incorporates a new Exhibit, reflecting the Investigator Badge utilized by personnel at the National Institute of Standard and Technology operating under the authorities specified in Section 2.04b and 2.04c. The language in Section 2.06 was revised to include the Special Agent delegation pursuant to 40 U.S.C. §1315. Section 7.09 was revised to include the addition of language authorizing actions by the Issuing official for unserviceable credentials.

SECTION 2. AUTHORITY.

.01 The Form CD-277, Official Credential, shall be used by the offices listed in paragraphs 2.03, 2.04, 2.05, 2.06, and 2.07 below, for the authority specified. The position designation for law enforcement officer or police officer positions shall be high risk or critical sensitive if access to National Security Information is required. Employees selected for such positions shall not receive the Form CD-277 and Badge until the appropriate background investigation has been successfully adjudicated and documentation has been verified that the employee has successfully completed training in: 1) basic law enforcement; 2) weapons qualifications; and 3) deadly force policy. The position designation for non-law enforcement officer or police officer positions shall be determined by the risk or sensitivity level of the position itself.

.02 A badge shall be issued according to the position held by the employee, as follows:

a. The Official Special Agent Badge shall be used only by those employees who are assigned law enforcement duties and responsibilities specified in paragraph 2.03 below.

b. The Official Investigator Badge shall be used only by those employees listed in paragraph 2.04 below who are required to perform official non-law enforcement investigations that must be coordinated with law enforcement agencies.

c. The Official Enforcement Officer Badge shall be used only by those employees who are assigned law enforcement duties and responsibilities enumerated in paragraph 2.05 below.

d. The Official Police Officer Badge shall be used only by those employees who are assigned police officer duties and responsibilities listed in paragraph 2.06 below.

e. The Undesignated Badge may be used only by select employees who are required to perform official security duties, inquiries, or other non-statutory Departmental administrative actions enumerated in paragraph 2.07 below.

.03 Only those employees who have been assigned law enforcement duties as specified in a statement of authorities below shall receive the Form CD-277 and Special Agent Badge.

a. Special Agents of the National Marine Fisheries Service, National Oceanic and Atmospheric Administration shall be issued the Form CD-277 and Special Agent Badge to perform all duties conferred upon them under the laws and regulations of the United States and the Department, including the authority to investigate, apply for and execute search warrants, serve subpoenas and summonses, administer oaths, make arrests without warrant, make seizures of property subject to forfeiture, bear firearms, and require and receive information on matters regarding the laws and regulations of the United States and the Department.

b. Special Agents of the Office of Inspector General shall be issued the Form CD-277 and Special Agent Badge to perform all duties conferred upon them by the Inspector General Act of 1978, as amended, and in accordance with the laws and regulations of the United States and the Department, including the authority to conduct criminal and other investigations, bear firearms, execute warrants, serve subpoenas, administer oaths, make arrests for offenses against the United States, and perform such other duties as are authorized by law.

c. Special Agents of Export Enforcement, Bureau of Industry and Security shall be issued the Form CD-277 and Special Agent Badge to perform all duties conferred upon them under the laws and regulations of the United States and the Department, including the authority to investigate, apply for and execute search warrants, serve subpoenas and summonses, administer oaths, make arrests without warrant, make seizures of property subject to forfeiture, bear firearms, and require and receive information on matters regarding the laws and regulations of the United States and the Department.

d. Special Agents of the Departmental Office of the Secretary assigned to and having been properly deputized for secretarial protection functions shall be issued the Form CD-277 and Special Agent Badge to perform all duties conferred upon them under the laws of the United States and the regulations of the Department, including the authority to protect the Secretary of Commerce, bear firearms, make arrests without warrant, and require and receive information on matters regarding the laws of the United States and the regulations of the Department.

e. Special Agents assigned to the Investigations and Threat Management Division [or Office, or Service, depending on the reorganization] shall be issued the Form CD-277 and Special Agent Badge to perform all duties conferred upon them under the laws of the United States and the regulations of the Department, and may exercise authority vested in the Secretary or otherwise provided to the [Division, or Office, or Service], including the authority to protect the Department's critical assets and activities, investigate, bear firearms, make arrests, administer oaths, apply for and execute legal process, and require and receive information on matters regarding the laws and regulations of the United States and the Department.

.04 Employees required to perform official non-law enforcement investigator duties as specified in a statement of authorities below shall be issued the Form CD-277 and Investigator Badge. Unless specifically noted otherwise, Investigators will be issued the Investigator Badge referenced in Exhibit 4

a. . Investigators of the Office of Inspector General shall be issued the Form CD-277 to perform all duties conferred upon them by the Inspector General Act of 1978, as amended, and in accordance with the laws and regulations of the United States and the Department, including the authority to conduct investigations and other inquiries, serve subpoenas, administer oaths, and require and receive information on matters regarding the laws and regulations of the United States and the Department.

b. . Security personnel in the Departmental Office of Security who have been formally trained via an approved course of instruction in investigative techniques/skills and currently performing in an official investigative capacity in support of a Departmental statutory function, shall be issued the Form CD-277 and Investigator Badge to perform all duties conferred upon them under the laws and regulations of the United States and the Department, including the authority to conduct investigations, make inquiries, administer oaths, coordinate with and obtain sensitive information from law enforcement organizations, and require and receive information on matters regarding the laws and regulations of the United States and the Department.

c. . Investigators of the National Institute of Standards and Technology, including the National Construction Safety Team (NCST), shall be issued the Form CD-277 and Investigator Badge (Exhibit 12) to perform all duties conferred upon them by the National Construction Safety Team Act, 15 U.S.C. 7301 et seq. and under the laws and regulations of the United States and the Department, including the ability to investigate building failures that resulted in substantial loss of life or that posed significant potential for substantial loss of life, access the site of a building failure being investigated, inspect any record, process of facility, inspect and test building components, materials and artifacts related to the building failure, and move the records, components, materials and artifacts related to the building failure.

d. Investigators of the National Institute of Standards and Technology performing investigations under NIST Organic Act authorities, shall be issued the Form CD-277 and Investigator Badge (Exhibit 12) to perform all duties conferred upon them under 15 U.S.C. 278f, 15 U.S.C. 281a, 15 U.S.C. 273, 15 U.S.C. 272(b)(11), 15 U.S.C. 272(c)(22) and the laws and regulations of the United States and the Department, including the authority to conduct investigations of fires, structural failures, and the performance of any activity authorized by the NIST Act, 15 U.S.C. 271 et seq.

e. . Compliance Officers of the Office of Antiboycott Compliance, Bureau of Industry and Security shall be issued the Form CD-277 and the Investigator Badge to perform all duties conferred upon them under the laws and regulations of the United States and the Department, including the authority to investigate, serve subpoenas, administer oaths, and require and receive information on matters regarding the laws and regulations of the United States and the Department.

.05 Enforcement Officers of the National Marine Fisheries Service, National Oceanic and Atmospheric Administration shall be issued the Form CD-277 and Enforcement Officer Badge to perform all duties conferred upon them under the laws and regulations of the United States and the Department, including the authority to investigate, apply for and execute search warrants, serve subpoenas and summonses, administer

oaths, make arrests without warrant, make seizures of property subject to forfeiture, bear firearms, and require and receive information on matters regarding the laws and regulations of the United States and the Department.

.06 Police Officers and employees with exclusive Special Agent designations delegated by the Director for Security, shall be issued the Form CD-277 and either a Police Officer or Special Agent Badge to perform all duties conferred upon them under the laws and regulations of the United DAO 207-11 - 4

-

2.07

States and the Department and bear firearms pursuant to 40 U.S.C. §1315 and 41 C.F.R. Part 102-72 and 102-81.

.07 When not otherwise covered by the Order, select employees throughout the Department, including those from the Departmental Office of Security, responsible for coordinating security functions with law enforcement and judicial organizations, may, at the sole discretion of the Director for Security, be issued the Form CD-277 and Undesignated Badge to perform required official inquiries or other non-statutory Departmental administrative actions including the authority to make inquiries, coordinate with and obtain sensitive information from law enforcement organizations, and require and receive information on matters regarding the laws and regulations of the United States and the Department.

.08 Employees required to perform official non-law enforcement duties as specified in a statement of authorities below shall be issued the Form CD-277 without a badge.

a. Equal Employment Opportunity (EEO) Investigators of the Departmental Office of Civil Rights shall be issued the Form CD-277 to perform all duties conferred upon them under the laws and regulations of the United States and the Department, including the authority to investigate Equal Employment Opportunity complaints, administer oaths, and require and receive information on matters regarding the laws and regulations of the United States and the Department.

b. Designated employees of Export Enforcement, Bureau of Industry and Security performing analytical/liaison functions shall be issued the Form CD-277 to perform all duties conferred upon them under the laws and regulations of the United States and the Department, including the authority to gather intelligence, and require and receive information on matters regarding the laws and regulations of the United States and the Department.

c. . Auditors, inspectors, and evaluators of the Office of Inspector General, and other employees designated by the Inspector General shall be issued the Form CD-277 to perform all duties authorized by the Inspector General Act of 1978, as amended, and in accordance with the laws and regulations of the United States and the Department, including the authority to conduct audits, inspections, evaluations, investigations and other inquiries, serve subpoenas, administer oaths, and require and receive information relating to the laws and regulations of the United States and the Department.

d. . Emergency Response Team members of the National Telecommunications and Information Administration shall be issued the Form CD-277 to perform all duties conferred upon them under the laws and regulations of the United States and the Department, including the ability to enter immediately into a disaster area to support the mission of the National Communications System (NCS), and the

national security/emergency preparedness requirements, and require and receive information on matters regarding the laws and regulations of the United States and the Department.

e. Compliance Officers of the National Oceanic and Atmospheric Administration, including personnel of the Commercial Remote Sensing Compliance and Monitoring Program (CRSCMP) shall be issued the Form CD-277 to perform all duties conferred upon them under the laws and regulations of the United States and the Department, including the authority to investigate, inspect and audit, and require

and receive information on matters regarding the laws and regulations of the United States and the Department.

f.. Assistant Secretary Export Enforcement and Deputy Assistant Secretary (DAS) Export Enforcement of the Bureau of Industry and Security shall be issued the Form CD-277 to perform all duties conferred upon such office under the laws and regulations of the United States Department of Commerce, including overseeing the activities of Federal Law Enforcement Officers dedicated to the enforcement of export control laws and regulations of the United States and the Department. If the DAS is a career Law Enforcement Officer (i.e. GS-1811/1801) and such functions are clearly defined in both position description and performance plan, he/she may carry badge and credentials as defined in 2.03c.

g.. Intelligence Research Specialists in the Departmental Office of Security shall be issued the Form CD-277 to perform all duties conferred upon them under the laws and regulations of the United States and the Department, including the authority to perform sensitive research, advisory, or liaison services and provide and receive information on matters regarding national security and law enforcement interests with a nexus to the mission of the Department of Commerce.

h.. Information and Personnel Security Division staff in the Departmental Office of Security may be issued the Form CD-277 to perform all duties conferred upon them under the laws and regulations of the United States and the Department, including the authority to perform sensitive research, inquiries, or liaison services and provide and receive information on matters regarding personnel security and national security matters with a nexus to the mission of the Department of Commerce.

i. When not otherwise covered by the Order, employees serving as security specialists (i.e. ZA-0080) from the Departmental Office of Security, may be issued the Form CD-277 to perform required official inquiries or other non-statutory Departmental administrative actions including the authority to make inquiries, coordinate with and obtain sensitive information from law enforcement organizations, and require and receive information on matters regarding the laws and regulations of the United States and the Department.

SECTION 3. RESPONSIBILITY.

.01 In those cases where the Director for Security has assurance that the holder of the specific credentials has current clearances and training to effectively execute the requisite duties of the occupied position, he/she shall sign all Form CD-277s authorizing the bearer to carry out official law enforcement duties in the Office of Export Enforcement, the National Marine Fisheries Service, the National Institute

of Standards and Technology, Office of the Secretary, and the Office of Security. The Director for Security shall also sign Form CD-277s for non-law enforcement positions, as well as retired law enforcement officer credentials. The Inspector General shall sign all Form CD-277s in the Office of Inspector General, including retired law enforcement officer credentials.

.02 The Director for Security shall manage the distribution and control of Form CD-277s and badges and oversee their use throughout the Department. When notified by the office or offices affected, the Director for Security shall revise the Form CD-277s and badges as necessary to conform to current law and Departmental policy.

.03 The head of each office listed in paragraphs 2.03, 2.04, 2.05, 2.06, and 2.07 above, shall designate to the Director for Security official(s) who will have authority and responsibility for requesting, issuing, and controlling the Form CD-277s and badges for their respective unit to include Retired Credentials.

.04 The official(s) designated in paragraph 3.03 shall be responsible for the individual issuance of the Form CD-277 and badge in his/her respective unit as well as the vetting process and subsequent

submission of Exhibit 9, for the issuance of Retired Credentials. He or she shall ensure that the need for a Form CD-277 and badge or Exhibit 9 and Retired Credential has been clearly established in compliance with this Order.

SECTION 4. OFFICIAL CREDENTIAL, FORM CD-277, AND OFFICIAL BADGES.

.01 Form CD-277 is in two parts. The top half identifies the bearer by name, title, operating unit, and office or division. The bottom half displays the bearer's photograph and signature, the unit authority statement, a serial number, and the authorizing signature. Exhibit 1 of this Order displays a sample Form CD-277 with law enforcement authority. Exhibit 2 displays a sample Form CD-277 with non-law enforcement authority.

.02 Upon individual issuance to Special Agents and Investigators, the name and title of the bearer shall be printed on the top half of the Form CD-277 in the type style of Exhibits 1 and 2 of this Order.

.03 The Official Special Agent Badge (Exhibit 3) identifies the bearer as a Special Agent. The Official Investigator Badge (Exhibits 4 and 12) identifies the bearer as an Investigator. The Official Enforcement Officer Badge (Exhibit 5) identifies the bearer as an Enforcement Officer of the National Marine Fisheries Service. The Official Police Officer Badge (Exhibit 6) identifies the bearer as a Police Officer of the Office of Security, while the Official Police Officer Badge (Exhibit 7) identifies the bearer as a Police Officer of the National Institute of Standards and Technology. Exhibit 8 depicts the Undesignated Badge. Badges shall be serially numbered, or otherwise uniquely identifiable, and issued with the Form CD-277, unless excluded by this Order or by the Director for Security.

.04 The Form CD-277 and badge shall not be altered except as authorized by the Director for Security.

SECTION 5. ISSUANCE AND CONTROL.

.01 The Form CD-277 shall display proper titles and be issued only to Departmental personnel in those offices listed in paragraphs 2.03, 2.04, 2.05, 2.06, 2.07, and 2.08 unless authorized by the Director for Security.

.02 The Director for Security shall issue the Form CD-277 and badges in blocks as requested in writing by the official designated in paragraph 3.03 of this Order.

.03 The Form CD-277 shall be laminated to prevent alteration and inserted in a credential case.

.04 A record must be made of any issuance of the Form CD-277 and badge. An accountability register shall be maintained by the issuing official who includes the bearer's name, Form CD-277 and/or badge number, date of issuance, geographic area where the bearer is assigned, and final disposition of returned forms and badges. An inventory of all issuances shall be conducted semi-annually and an inventory report provided to the Director for Security annually by December 31. Any discrepancy discovered in the inventory shall be reported immediately to the Director for Security (see paragraph 7.05 below).

.05 Notwithstanding the provisions of paragraph 2.01 (i.e. weapons qualifications, etc.) the Director for Security may make badges/credentials available to those participating in Federal Law Enforcement Training Center (FLETC) basic law enforcement graduation ceremonies when the bureau's on-site representative attests that no known circumstances exist which would cause them to believe the individual would not obtain a FLETC diploma following the normal administrative period that traditionally exists (but not more than 2 weeks) to prepare/print/deliver certificates and all other requirements noted in this Order have been fully satisfied and documented. In these instances, certification of issuance or other credential dispensation is documented via Exhibit 9 which serves as a supplemental documentation to traditional requests.

.06 The issuing official shall ensure that personnel who are issued Form CD-277s and badges are properly informed as to the requirements and obligations governing such use under prescribed professional standards of conduct.

.07 The issuing official shall retain returned badges and cases for reissuance, and the returned Form CD-277s shall be destroyed or processed as unserviceable and returned to the employee (see paragraph 7.09 below).

.08 At the discretion of the head of each office listed in paragraph 2.03 of this Order, and consistent with policies and procedures established for each such office, Special Agent Badges may be issued in duplicate for use in operational situations where it would be unsafe or impractical to display the badge mounted in or on the Form CD-277 case.

SECTION 6. RETIRED LAW ENFORCEMENT OFFICER CREDENTIAL.

.01 The Office of Security shall issue a Retired Law Enforcement Officer Credential (Exhibit 10) to employees of the Department who retire or separate from federal service in good standing with the Department, after at least 10 years of aggregate service (or other appropriate provisions of Public Law 108-277 as validated by the designated official and others in the vetting offices) as a federal law enforcement officer or agent, (defined by paragraphs 2.03, 2.05 and 2.06), had no serious disciplinary problems during his/her service as a federal law enforcement officer or agent, and sign a certification (Exhibit 11) concerning the use and disposition of the Credential. The certification will include a provision under which the recipient of the Credential agrees to release, indemnify and hold harmless the United States Government, and any and all departments, agencies, or employees thereof, from any and all liability incurred as a result of any act or omission of the recipient arising out of or otherwise related to the issuance or use of the Credential.

.02 Prior to submitting the application (credential request form to include Exhibit 11) to the Office of Security for the authorization and approval by the Director for Security, the applicant must be vetted through the servicing Human Resources Office, Office of Inspector General and the Office of General Counsel.

.03 The official designated in paragraph 3.03 shall be responsible for the vetting process. He or she shall certify the need for a Retired Credential has been clearly established in compliance with this Order. In addition, he or she is responsible for properly coordinating the credential request form (to include Exhibit 11) through their servicing Human Resources Office, Office of Inspector General and the Office

of General Counsel. The vetting process is an opportunity for an Official from stated offices to review the application and indicate whether they are aware of information concerning the applicant that could

lead the Department to determine that the applicant did not separate in good standing and with no serious disciplinary problems during his or her service.

.04 For purposes of issuing a Retired Credential, an employee separated or separating from service may be considered not to have retired or separated in "good standing" if:

a. The employee separated during pending inquiry or investigation where the facts were likely to lead to a proposal for removal or other serious disciplinary action;

b. The employee separated following an inquiry or investigation leading to a determination that the employee had engaged in misconduct that could result in a proposal for removal or other serious disciplinary action but before any such action had been proposed;

c. The employee separated following a proposal or decision to remove the employee;

d. The employee had his/her security clearance suspended or revoked at the time of separation;

e. The employee has been officially found by a qualified medical professional employed by the agency, to be unqualified for reasons relating to mental health or otherwise had been found to be not fit for duty;

f. The employee had serious disciplinary problems during their service as a federal law enforcement officer; or

g. There is a situation or circumstance (other than those listed) that is deemed in the discretion of a Department office, or the Director for Security, not to constitute "good standing.".

.05 The Retired Credential shall be issued only on the written recommendation of the Department operating unit by which such employee was employed at the time of his or her separation, and only if meeting the above stated criteria. It is recommended that two officials – the Head of the Operating Unit and another official between the applicant and the Head of the Operating Unit in the chain of command – certify that the applicant should be approved.

.06 Retired Credentials shall remain the property of the Department of Commerce and must be surrendered upon request.

SECTION 7. USE AND DISPOSITION.

.01 The Form CD-277 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. The Form CD-277 and badge shall not be used as a building pass. Penalties may be imposed pursuant to law for the improper use of official identification (see 18 U.S.C. §§ 499, 701, and 1028).

.02 Individuals are personally responsible for safeguarding authorized Form CD-277s and badges from loss, theft, or possible misappropriation by any means while minimizing personal risk. The Form

CD-277 and badge shall remain in the bearer's personal possession and not be left or stored in a manner which allows access by unauthorized persons. When not being used for a period of time, or when the bearer is on extended leave, the Form CD-277 and badge shall be secured in a government security container or locked file cabinet.

.03 Both parts of the Form CD-277 shall be carried in a plain black folding case having clear windows inside to permit reading of the two halves of the Form CD-277 in the case.

.04 Except with respect to duplicate Special Agent Badges issued in accordance with paragraph 5.07 of this Order, the Special Agent, Enforcement Officer, Investigator and Undesignated badge should be mounted in or on the case holding the Form CD-277 Official Credential. Further, Form CD-277 Official Credential should be maintained on the individual at any time a badge is donned, however, unless procedures and guidelines for public display of these badges are further established by the head of the office listed in paragraphs 2.03, 2.04, 2.05, 2.06 or 2.07 of this Order.

.05 Loss or theft of, or damage to, credentials and badges shall be immediately reported in writing to the issuing official with an explanation of the circumstances. An investigation into the circumstances concerning the loss, theft, or damage shall be immediately conducted by the issuing official. A copy of the report, which identifies the bearer's name, credential, badge number, date and place where the incident occurred, and other relevant facts, shall be forwarded to the Director for Security within 30 days after the completion of the investigation but no more than three months after the date of the loss, theft, or damage. Lost or stolen badges and credentials must be entered into the National Crime Information Center (NCIC) by the Operating Unit. Recovered credentials and badges are to be reported to the issuing official without unreasonable delay, and accountability records shall be adjusted to reflect the recovery. Recovered credentials may be either destroyed or reissued to the bearer, as appropriate. Under no circumstance, however, are individuals to retain more than one Form CD-277 at a time.

.06 Loss or theft of Retired Credentials shall be immediately reported to local police authorities with a request that an investigation be initiated and the loss or theft be entered into the NCIC. Any request to replace the lost or stolen Retired Credentials must be accompanied by a copy of an investigative report. A one-time replacement may be issued at the discretion of the Office of Security at no cost to the separated individual.

.07 Unless otherwise determined by the person designated in Section 2.03, credentials remain valid for the duration of employment, and once issued, are not to be reissued merely because of a change in the name or title of the authenticating official. Credentials shall be updated and reissued to the bearer when a change takes place under the following conditions:

a. Legal name change;

b. Official reassignment to a different position to reflect a change in title or in the bearer's authority; or

c. Mutilation of the credential, excessive wear, or lapse of sufficient time to indicate that a lost or stolen Form CD-277 will not be returned or recovered.

.08 Records shall be maintained by designated issuing officials to indicate the disposition of all credentials and badges. Upon termination of employment, reassignment, or transfer, the bearer shall return the Form CD-277, badge, and case to the issuing official prior to being granted final separation clearance. Issuing officials shall take appropriate action to ensure that credentials and badges are returned, or otherwise accounted for, prior to the employee separating from the service or the Department or transferring to another organizational unit within the Department.

.09
Credentials of employees who retire or separate may be held for a period of time and then destroyed, or otherwise be made unserviceable and returned to the individual upon a minimum of one year of continuous service at the discretion of the issuing official. Unserviceable credentials authorized for return to separating employees shall not be used as official identification, proof of service, or to obtain government benefits. Badges will not be used as mementos to employees separating from service and shall be returned to inventory for re-issuing.

.10 The careless handling, abuse, misuse, or intentional misrepresentation of official credentials and badges shall be cause for possible administrative or disciplinary action.

SECTION 8. EFFECT ON OTHER ORDERS.

This Order supersedes Department Administrative Order 207-11, dated July 11, 2008.

_____

Deputy Secretary of Commerce

COPIES OF THE EXHIBITS CAN BE OBTAINED FROM THE OFFICE OF SECURITY

U.S. Department of Commerce
Office of Security
Investigations and Threat Management Division

INVESTIGATIVE PLAN

CONTROL NUMBER:

[Insert TMT/CNET number]

DATE:

[Insert date you submitted this IP for review]

ASSIGNMENT TYPE:

[CI-TOC/EE-CT-Other; for PI use the Assessment Record instead of an IP]

AFFECTED OFFENSE/REGULATION:

[For threats which are yet uncognizable as criminal offenses insert the following: **Department Organization Order 20-6**]

[For cognizable criminal offenses or policy/regulation violations, insert applicable **statute or regulation number**]

ITERATION:

[Insert this IP's version number]

PERIOD COVERED:

[Insert dates from last IP version to present. i.e. 12 July 2014 – 2 August 2014]

THREAT CATEGORY:

[Insert as applicable, based on best evidence to date:

- Category I – Imminent Threat
- Category II – Cognizable Threat
- Category III – Potential Threat
- Category IV – Undetermined Threat]

RISK SCORE:

[Insert as applicable, based on best evidence to date against DOC Risk Scoring Matrix:

- HIGH
- MODERATE
- LOW]

BASIS:

[Insert accurate, complete and concise basis for investigation as known from Report of Inquiry]

PLAN:

ACTION

[TECHNIQUE: best evidence yielded to date. *TECHNIQUE: next step to reduce presumption and ambiguity. TECHNIQUE: next step to reduce presumption and ambiguity.* Etc.]

[TECHNIQUE: next best evidence yielded to date. *TECHNIQUE: next step to reduce presumption and ambiguity. TECHNIQUE: next step to reduce presumption and ambiguity.* Etc.]

[Etc.]

NEXUS

[TECHNIQUE: best evidence yielded to date. *TECHNIQUE: next step to reduce presumption and ambiguity. TECHNIQUE: next step to reduce presumption and ambiguity.* Etc.]

[TECHNIQUE: next best evidence yielded to date. *TECHNIQUE: next step to reduce presumption and ambiguity. TECHNIQUE: next step to reduce presumption and ambiguity.* Etc.]

[Etc.]

VALUE

[TECHNIQUE: best evidence yielded to date. *TECHNIQUE: next step to reduce presumption and ambiguity. TECHNIQUE: next step to reduce presumption and ambiguity.* Etc.]

[TECHNIQUE: next best evidence yielded to date. *TECHNIQUE: next step to reduce presumption and ambiguity. TECHNIQUE: next step to reduce presumption and ambiguity.* Etc.]

[Etc.]

ATTACHMENTS:

[Always reference Activity Notes and the corresponding completed Report of Inquiry, as well as any investigative adjuncts. Insert document title(s) and location(s), if applicable, e.g. Operations Order #01//File #2000876]

REMARKS:

[Insert as applicable:

- Any remarks regarding a need to elevate a specific investigative technique due to urgent circumstances.
- Any remarks regarding immaterial discrepancies.
- Any remarks regarding administrative factors that impacted the investigation, including reasons for any deadline extensions and any information that was unobtainable.
- Any procedural contributing factors and corresponding recommendations for corrective action.]

REVIEW:

[Reserved for supervisor comment, if necessary]

CERTIFICATION AND APPROVAL:

_____
Agent Signature/Date

_____
Supervisor Signature/Date

Next Review: _____
Date

DISTRIBUTION:

[Insert distribution (other than CNET or working laptop), if applicable]

Thirty-five (35) Pages Withheld In Full Pursuant to (B)(7)(E)

SPECIAL AGENT DIRECTIVE

Appendix 1

Name: Use of Force and Weapons

Effective Date: 09/08/2017

PURPOSE: To require US Department of Commerce (DOC) Special Agents (Agents) under Office of Security (OSY) policy authority to use force and bear weapons in an effective and responsible manner. Nothing in this directive or in its appendices or attachments is intended to create, nor does it create, an enforceable legal right or private right of action.

POLICY: All Agents must follow the requirements within this directive in order to exercise the authority to use force and employ weapons as a federal law enforcement officer.

I. **Use of Force.** Agents may be required to use force in order to effectively exercise law enforcement authority. Agents who use force (including the use of weapons) for law enforcement purposes will conform to United States Marshals Service (USMS) Use of Force requirements. The use of force by an Agent must be objectively reasonable and may range from verbal commands to deadly force. Force may also be used against animals when necessary in self-defense or in defense of others.

A. **Less-Than-Lethal Force.** Less-than-lethal force is force that is neither likely nor intended to cause death or serious physical injury. Agents may use less-than-lethal force only in situations where reasonable force, based upon the totality of the circumstances at the time of the incident, is necessary to protect themselves or others from physical harm; restrain or subdue a resistant detainee or suspect; prevent a detainee from escaping; make an arrest; or otherwise obtain lawful compliance from a subject. Choke holds, carotid-control holds, or other neck restraint associated with the use of less-than-lethal force are prohibited absent exigent circumstances.

1. Less-Than-Lethal Devices. Issued less-than-lethal devices (Oleoresin Capsicum (OC) spray or tactical baton) may be used on an active resistant subject in situations where verbal commands or persuasion are not or would not be effective and the subject's actions demonstrate that physical control by the Agent is not or would not be effective. Absent exigent circumstances, implementation of less-than-lethal devices in deadly force situations is not recommended and less-than-lethal devices should not be substituted for a firearm.

a. *Device Prohibitions.* Agents are not authorized to use less-than-lethal devices if voice commands or physical control achieve the law enforcement objective. Agents using a less-than-lethal device must stop using the device once it is no longer needed to achieve the law enforcement purpose for which it is being used. Less-than-lethal weapons may not be used to punish, harass, taunt, or abuse a subject. Use of baton to apply choke or "come-along" holds to the neck area and intentional strikes with a baton to the head/face, neck, spinal column, solar plexus, kidneys, groin, or joints are prohibited absent exigent circumstances.

B. **Deadly Force.** Deadly force is the use of any force that is likely to cause death, or serious physical injury (serious/permanent disfigurement or loss of function of a body part or organ). Agents may use deadly force only when they have a reasonable belief that the subject of such force poses imminent danger of death or serious physical injury to the Agent or to another person.

1. If feasible, and if doing so would not increase the danger to the Agent or others, a verbal warning to submit to the authority of the Agent shall be given prior to the use of deadly force.

2. Deadly force may not be used solely to prevent the escape of a fleeing suspect or an escaping detainee. An Agent may use deadly force against a fleeing suspect or escaping detainee only when the Agent has probable cause that the suspect or detainee poses an imminent danger of death or serious physical injury to the Agent or to another person.

3. Warning shots are not permitted outside of the prison context.

4. Firearms may not be fired solely to disable moving vehicles.

C. **Injuries.** In all use of force incidents, Agents must make necessary medical assistance available to subjects as soon as practicable. Any injury to an Agent or another party must be documented and reported as soon as practicable to the Agent's supervisor, who must notify the DOC Emergency Operations Center (EOC) as soon as possible. Once a subject and scene have been controlled and properly secured, Agents should attempt to document in the best manner possible any marks or alleged injuries resulting from the use of force. If the marks or alleged injuries to be documented are on a private portion of the subject's body, Agents will ensure privacy before preparing documentation. For arrestees, Agents will notify the appropriate detention facility if a subject has been injured and/or received medical attention.

1. External Investigation or Assistance. For deadly force incidents, managers will, as appropriate and in consultation with the Office of General Counsel, promptly request another law enforcement agency with jurisdiction assume control over the scene and conduct an investigation involving the incident. For matters that do not involve deadly force, the involved Agent while on scene, another Agent on scene, or the involved Agent's supervisor or manager may request assistance from another law enforcement agency with jurisdiction to assist with securing the scene, providing medical assistance, and/or documenting alleged use of force injuries.

D. **Incident Reporting.** With the exception of simple commands that result in compliance, Agents must verbally report all use of force incidents to their supervisor as soon as possible, and must subsequently prepare and submit a written report within 3 business days.

1. Administrative Review Board. When an Agent acting in their official capacity has used force which caused serious bodily injury or death, an administrative review will occur to determine if the Agent acted in accordance with the provisions of this directive.

a. *Purpose.* The Review Board will determine whether use of force was authorized and in accordance with this directive, but will not decide if discipline is merited. The Review Board may recommend changes to this directive which could mitigate risk in future use of force situations.

i. The Review Board may not evaluate the appropriateness of use of force unless any investigation conducted by a law enforcement agency over the incident has concluded, and a declination of prosecution has been obtained. However, risk mitigation analysis and recommendations may occur if the investigating agency provides sufficient facts to evaluate and

concurs with the need for analysis and recommendations prior to the conclusion of any criminal investigation.

b. *Composition.* The Review Board will be composed of a federal law enforcement officer from a DOC operating unit and a federal law enforcement officer from an external US Government agency, both with at least 5 years of current, full-time law enforcement experience; the Firearms Instructor who most recently qualified the employee; the Control Tactics Instructor who most recently trained the employee; and a representative from the Office of General Counsel, who will convene the Board.

c. *Basis.* The Review Board will obtain a copy of the investigating law enforcement agency's report, or if unavailable request that the DOC Office of Inspector General conduct an inquiry to ascertain the facts of the incident. Agents whose actions are under the Review Board's purview may submit a written explanation at any time of any matter relevant to the Board's deliberations.

d. *Findings.* A review is concluded when a unanimous decision has been reached by the Board members. Within 10 business days of concluding a review, the Board will submit completed reports to the Office of General Counsel. After Office of General Counsel review, the Board will submit a final report to the Director for Security, the Agent's manager, and the Agent.

II. **Arming Authorization.** Before being authorized to carry and use a weapon, an employee must meet all qualifications for employment as an Agent, and be deputized by the USMS (or otherwise vested with applicable law enforcement authority). Weapons are issued or assigned to Agents for their exclusive use, except for use by another law enforcement officer with proper jurisdiction during an emergency.

A. **Lautenberg Amendment.** Pursuant to 18 USC 922, no one convicted in any court of a misdemeanor crime of domestic violence is eligible to carry a firearm unless the conviction is expunged, set aside, or the individual receives a pardon.

1. All Agents will annually provide a signed, sworn statement that they have not been so convicted. If any Agent is convicted of such a crime while in service, they must immediately report this to their supervisor. Supervisors will ensure that a convicted employee immediately surrenders all issued weapon(s).

B. **Retired Agents.** Eligibility to carry firearms by retired Agents under 18 USC 926 is subject to the provisions of Department Administrative Order 207-11.

III. **Proficiency.** As a condition of employment, Agents are required to demonstrate proficiency to an instructor on a semi-annual basis, which includes the ability to properly operate all authorized weapons in a safe, efficient, and effective manner. Authorized weapons will be carried and used in a manner consistent with current training procedures as established during the Agent's most recent training session.

A. **Firearms.** Agents will qualify on a Federal Law Enforcement Training Center (FLETC) range, but may qualify at another facility designed for firearms use if FLETC is unable to reasonably schedule a session, or if the Agent's duty station is not within a reasonable commuting distance of a FLETC range. The standard for qualification will be the same for all Agents, and all scores will be recorded as pass or fail. During normal duty hours, a DOC Firearms Instructor will oversee all firearms qualifications, to include ensuring that Agents receive a use of force, safety, and familiarization briefing prior to firing. Prior to qualification, a Firearms Instructor or armorer will inspect each firearm to ensure working order. DOC or FLETC Firearms Instructors must personally observe all qualifications, score targets, and record scores on a Firearms Qualification

and Certification Record. DOC Firearms Instructors cannot self-qualify. The wearing of body armor is encouraged. Non-law enforcement personnel may not be present on the firing line.

1. Handguns. All Agents must qualify cold bore (without practice immediately before qualification) on an appropriate qualification course found in Attachment I. Agents will train and qualify only with holsters authorized by this directive.

    a. To promote firearms proficiency, Agents may use assigned handgun(s) under proper arming authorization for practice at a facility designed for firearms use. Agents may be issued up to 500 rounds per fiscal year, and will not be reimbursed for any other associated costs (including range fees). Any ammunition purchased at the Agent's own expense must be factory loaded, commercially available ammunition produced by a major manufacturer. Agents solely incur any and all liability as a result of their actions associated with private practice with their handgun(s).

2. Long Arms. Agents assigned to deploy carbines and who have been issued a personally sighted carbine must qualify quarterly cold bore on an appropriate qualification course found in Attachment I; for carbines equipped with optics, Agents must alternate qualification with optics and iron sights per quarter. Agents authorized to deploy shotguns must complete an appropriate qualification course found in Attachment I cold bore semi-annually.

3. Annual Familiarization Training. Agents must complete annual clearing and malfunction drills, low light firearms drills, moving and shooting drills, and downed/disabled drills with all issued firearms, as well as non-lethal training ammunition exercises for familiarization purposes.

4. Failure to Attend Qualification. Supervisors will counsel Agents in writing and secure issued firearm(s), credentials and badge from Agents who fail to attend 2 consecutive quarterly firearms qualification sessions. Firearms will be returned after the Agent has successfully demonstrated proficiency.

    a. Failing to attend 2 consecutive qualification sessions due to supervisor-assigned work will not result in written counseling. In such instances, a written memorandum explaining the circumstances will be prepared by the supervisor and forwarded to the manager for review.

5. Failure to Qualify. If an Agent fails to qualify with an issued firearm after 2 consecutive attempts in a single session, the supervisor will secure the Agent's firearm, credentials and badge. Supervisors will provide the firearm to an armorer for inspection if the instructor believes there is a mechanical malfunction; if an armorer determines there is a mechanical malfunction, the Agent will be returned their credentials and badge, and scheduled for requalification (after repair or replacement of the firearm) within 1 week.

    a. If an instructor did not suspect a mechanical malfunction or if no mechanical malfunction was detected, the Agent will be counseled in writing by their supervisor, scheduled for 1 session of the FLETC Marksmanship Enhancement Training Program, and within 1 week of completion be provided another opportunity to qualify. An Agent will not be permitted to carry any weapon and will be placed on limited duty during this period.

    b. Failure to qualify again will result in repeating the above process.

c. Agents that fail to qualify after completing this second iteration (or within 1 year from the quarter of their last successful qualification after remediation) will be processed for administrative action according to

DOC Office of Human Resources Management policies, while Agents who successfully achieve a qualifying score after remediation will be returned their handgun, credentials and badge.

B. **Less-Than-Lethal Devices.** On a semi-annual basis, Agents demonstrate proficiency with less-than-lethal devices via a practical and written evaluation administered and documented by a Control Tactics Instructor. Agents that fail to demonstrate proficiency will receive remedial training necessary to attain certification before being permitted to possess, carry or use the weapon.

C. **Allied Competencies.** Agents will be trained on a semi-annual basis in alternative methods and tactics for addressing a resistant subject, which must be used when the use of deadly force is not authorized by this directive. In addition to instruction in the use of less-than-lethal weapons, Control Tactics Instructors will provide refresher training in weapons retention, handcuffing, and addressing passive and active resistance without weapons. Tactics Instructors will provide semi-annual refresher training in basic tactics.

IV. **Weapons Carriage and Use.** Agents are authorized to carry weapons in order to perform official duties. Carriage to perform official duties is defined as an Agent's scheduled work hours, unscheduled overtime, and any time an Agent in the 1811 job series is subject to availability, or any time an Agent in the 0080 job series is subject to immediate recall. Agents will carry all weapons concealed when in public, unless a law enforcement or training circumstance dictate otherwise. Agents will carry their credentials (Form CD-277) and badge when possessing a weapon, except when the discovery of credentials might compromise the success of a particular mission and this has been documented in advance by the supervisor. Agents will not surrender any weapon unless relieved by proper authority. Managers will establish rules regulating weapons carriage within the office, depending upon the need for immediate access and each office's security features. All authorized firearms must be carried and used in accordance with applicable federal law and regulation.

A. **Firearms.** Agents will treat all firearms as if they are loaded, and no firearm will be inspected or cleaned without being properly cleared of ammunition. All Agents are required to immediately report to their supervisor any knowledge of a gross safety violation, malfunction, or unintentional discharge involving an authorized firearm. Agents may not consume alcohol while carrying a firearm, or for at least 8 hours prior to carriage. Agents shall not carry a firearm while taking medication that may impair their judgment and/or ability to safely control a firearm. Whenever carrying an authorized firearm, when directed by a supervisor Agents will also carry spare magazines (or equivalent) and a restraining device.

1. Handguns. During an Agent's scheduled work hours or unscheduled overtime, all Agents authorized to carry firearms will carry or have readily accessible an assigned handgun. Agents shall carry assigned handguns with a chambered round and full magazine. Based on specific circumstances, supervisors may authorize in advance the carriage of more than one handgun as prudent.

a. *Enforcement and Routine Activities.* For enforcement activities (acts of arrest, search, or seizure), Agents are required to carry at minimum an assigned compact firearm listed in Attachment I. For routine activities, in order to better meet operational needs Agents may carry an assigned sub-compact firearm listed in Attachment I.

b. *Personally Owned Handguns.* In accordance with all other provisions of this directive, with a manager's written approval Agents are authorized to carry a personally owned handgun that meets specifications listed in

Attachment I in lieu of the assigned handgun, in order to satisfy operational needs and to better ensure agent safety.

i. Authorization to carry personally owned handguns is subject to specific mission needs on a case-by case basis, or for carry when subject to availability or immediate recall. Managers must cite the specific mission need (with a corresponding approved timeframe) or blanket availability/recall authorization in their written approval.

ii. Personally owned handguns must be the manufacturer's original design, specifications, and function.

iii. Personally owned handguns must be obtained and maintained at the Agent's own expense, including expenses for demonstrating proficiency.

c. *LEOSA*. Agents who choose to carry a personally owned firearm under the Law Enforcement Officers Safety Act (18 USC 926B) or in accordance with the laws of a state do so outside the scope of employment and must independently meet any related requirements; carrying firearms under these provisions is in a personal capacity, is not under the authority of DOC, OSY or the USMS, and does not confer law enforcement powers.

2. Long Arms. Agents are authorized to employ issued long arms when performing their official duties based upon the situation and their perception of the level of threat. Supervisors may overrule the decision to employ long arms if they reasonably believe the situation does not justify use. Issued long arms will be stored in an office and are not approved for routine carriage, or travel to or from an Agent's residence. Long arms must be carried with the safety engaged and an empty chamber on a full magazine with the bolt forward (duty carry) until deployed against a potential danger; once the Agent perceives the potential for a threat, long arms will have a chambered round with the firearm on safe (hot carry) until the Agent is immediately prepared to engage a threat.

a. *Selective Fire*. Managers may authorize carbines capable of selective fire. Authorization must be based on specific special operations, and discretion will be used in determining which Agents will be assigned these weapons. Agents assigned selective fire carbines must first complete an additional 8 hours of proficiency training with each assigned weapon system that is provided by a Firearms Instructor trained by FLETC in the use of fully automatic or burst fire weapons.

B. **Carriage Aboard Commercial Airlines.** When under proper arming authorization, Agents that use commercial aircraft to travel may be armed and immediately prepared for duty pursuant to Title 49, Code of Federal Regulations (CFR), Section 1544.219 and applicable Federal Aviation Administration (FAA) regulations. Agents will keep weapons within their immediate control, and out of view of passengers and crew. Agents will not surrender their handgun to aircrew at any time. While in the cabin of the aircraft, in the event of an in-flight incident that is not associated with the Agent's official duties, Agents will not intervene unless an imminent threat of death or serious physical injury exists, or assistance is requested by a crew member or Federal Air Marshal.

1. Administrative Requirements. Agents must annually complete the Transportation Security Administration's (TSA) Law Enforcement Officers Flying Armed course taught by a Firearms Instructor, and upon successful completion will receive a Law Enforcement Officers Flying Armed Training Certification. Managers will ensure TSA

security codes are distributed to Agents in a timely manner. Agents are required to complete the airline's authorization forms.

2. Handguns. No authorized handguns will be transported in checked baggage.

3. Long Arms and Bulk Ammunition. After approval by a supervisor, all issued long arms will be transported in checked baggage, along with any ammunition that is not loaded in an Agent's handgun or corresponding spare magazines. Long arms must be unloaded

   and stored in a suitable hard-sided container that is locked by combination or key (this container may be secured within another piece of luggage to be less conspicuous and to prevent theft); bulk ammunition must be stored in similar fashion in a separate container. If possible, Agents will pre-check long arms and bulk ammunition with TSA the day before travel; if not possible, Agents will declare to the airline at the time the bag is checked that the bag contains an unloaded firearm and/or bulk ammunition. Agents will ensure that the firearms tag or other tag provided by the airline is placed inside the shipping container.

4. Less-Than-Lethal Devices. Tactical batons may be transported on the Agent's person or in carry-on baggage, and will remain under the Agent's control at all times. Agents are not permitted to carry OC spray on board any commercial aircraft, but may check OC spray in limited quantities pursuant to FAA, TSA and carrier regulations.

5. Denial. If an airline will not allow an Agent to board an aircraft armed, Agents must contact their supervisor and speak with the airport's Ground Security Coordinator. If they are still denied boarding while armed, supervisors will determine whether and when mission needs require the Agent to take another flight, and will notify a manager within 1 business day for reporting of the incident to the Federal Aviation Administration.

C. **Carriage Aboard Private Aircraft.** Agents carrying firearm(s) domestically aboard private aircraft or at private airports must contact the carrier or airfield and make any necessary arrangements as applicable.

D. **Carriage in or Transit through Foreign Countries.** After a manager's approval, Agents must obtain advance written permission to possess a weapon in a foreign country from the country's respective legal authority through the Department of State – Regional Security Officer, or if applicable through an appropriate US military authority.

E. **Less-Than-Lethal Devices.** As permitted by law or regulation, Agents are encouraged to carry OC spray or a tactical baton as an additional force option in order to perform official duties. Supervisors may order an Agent under their command to carry one or more less-than-lethal devices, based on mission requirements. Agents engaged in enforcement activities as defined in this directive are required to carry at least 1 less-than-lethal device. When carried, less-than-lethal devices will be secured in a manner to prevent unintentional deployment.

1. OC Spray. Agents will avoid using OC spray, if possible, under conditions where it may affect innocent bystanders. Whenever practical and reasonable, personnel should issue a verbal warning prior to using OC, be upwind from the offender, and deploy the spray no closer than 2 feet at the offender's eyes, nose and mouth. A second burst, if necessary, should be aimed towards the nose and mouth only. Agents will cease OC usage once the offender's compliance is gained or it is obvious the OC is ineffective. OC spray should not be stored near heat or flame, deployed near sparks or flames, nor kept in a motor vehicle or any area where extremely high or low temperatures are likely to occur. Agents will use an OC canister only once; after discharge, Agents will turn the canister into their supervisor.

2. Tactical Baton. Agents should use tactical batons to strike attacking limbs (arms, hands, legs, and feet) and/or large muscle groups, but unless deadly force is necessary will not use batons to strike the head, neck, or spine, or the solar plexus, kidneys, groin or joints. Agents will not employ batons as compliance tools.

V. **Weapons Security.** Agents are personally responsible for preventing the inappropriate display, unauthorized handling, or unintentional discharge of authorized weapons. All authorized firearms must be stored and maintained in accordance with applicable federal law and regulation. An Agent absent from official duties for more than 30 days will be required to surrender issued weapons to their supervisor for safekeeping.

A. **Unattended Weapons.** Agents will not leave any authorized weapon unattended, unless the weapon is secured in accordance with this directive. While performing official duties, Agents may provide their weapon(s) to another law enforcement officer that is armed for safekeeping at the direction of a supervisor, when operational circumstances outside of the office require unarmed activities, or whenever the Agent recognizes the unanticipated onset of personal issues that may imminently impair their ability to secure their own weapon(s). If another law enforcement officer cannot secure the Agent's weapon(s), the Agent is required to secure weapon(s) by reasonable and prudent measures in order to prevent unauthorized access.

1. Firearms. When not performing official duties and not under their immediate control, Agents may either store their handgun in an office gun vault, or if outside of the office render the gun inoperable by unloading the firearm, securely storing the ammunition separately from the firearm, and installing an issued trigger lock; alternately, an Agent's handgun may be secured in a locked container designed for firearms storage to which only the Agent has access.

2. Less-Than-Lethal Devices. When not performing official duties and not under their immediate control, Agents will store less-than-lethal devices in a locked container to which only the Agent has access.

B. **Office Storage.** Offices staffed by Agents will contain a gun vault, a commercially manufactured bullet trap capable of containing a standard rifle cartridge discharge, and instructions for making safe commonly encountered firearms.

1. Firearms. While performing official duties, handguns may be temporarily stored loaded and ready for immediate use (chambered round and full magazine) in locked containers to which only the Agent has access. Firearms not in use will be stored unloaded (with the safety on for models with this feature) in a locked gun vault.

2. Less-Than-Lethal Devices. Less-than-lethal weapons will be stored within the Agent's workspace in a locked but readily accessible container to which only the Agent has access.

C. **Inventory.** A supervisor in conjunction with an instructor or armorer will conduct a monthly inventory of issued weapons by personally verifying the presence of items against property receipts.

D. **Shipping Weapons.** All weapons will be shipped in accordance with federal law and regulation. Weapons will be insured by traceable courier using "Priority Overnight" service, sent only on a work day when overnight delivery can be accomplished, securely packed in an unmarked box to prevent their movement during shipment, and for firearms cleaned and unloaded.

E. **Loss, Theft or Damage of Weapon.** Agents will immediately report the loss, theft or damage of any issued weapon (including ammunition and accessories) to their supervisor, and for loss or theft to the EOC and a law enforcement agency of the jurisdiction where the incident occurred. Within 24 hours of an Agent's report, supervisors will notify the Property Custodian. Managers will ensure that a stolen item is entered into and remains in NCIC unless recovered. Managers

shall ensure that an appropriate inquiry is made to determine culpability, if any, for the loss, theft or damage of an issued weapon. When an issued weapon is lost, stolen or damaged due to an Agent's negligence, the Agent may be required to pay for the item and may also be subject to disciplinary action.

F. **Unintentional Discharge.** Any Agent who witnesses an unintentional discharge of a firearm is required to immediately report the incident to their supervisor. Supervisors must secure involved firearm(s) and the scene of the incident, provide any necessary medical assistance, and immediately inform as appropriate any law enforcement agency which may respond to reports of the incident. Supervisors must also report the incident to the EOC. The Administrative Review Board will review all unintentional discharges.

VI. **Authorized Equipment and Serviceability.** Special Agents may only possess, carry or use authorized and serviceable weapons, ammunition, and accessories under OSY policy authority.

A. **Firearms.** A description of authorized firearms can be found in this directive's Attachment I. Operating units will maintain at least 1 spare handgun for sidearms that are not available for use, and will have a minimum ratio of 1 long arm for every 3 Agents in order to meet operational needs.

1. Ammunition. A description of authorized ammunition can be found in this directive's Attachment I. Only factory loaded, commercially available ammunition produced by a major manufacturer is authorized for use in issued firearms; Excessed (but not abandoned or forfeited) ammunition may be used only when in accordance with current USMS policies. Issued ammunition must have been favorably evaluated by the Federal Bureau of Investigation's Firearms Training Unit. All training ammunition is required to be the same ammunition used for duty. Agents will be issued fresh ammunition for duty by a Firearms Instructor after each successful qualification session, and will inspect ammunition every time they load or unload; any ammunition that appears corroded, dented, deformed, cracked or broken will be immediately removed from service and returned to the issuing Firearms Instructor. Agents will not modify ammunition in any way.

B. **Less-Than-Lethal Devices.** A description of authorized less-than-lethal devices can be found in this directive's Attachment I.

C. **Accessories.** Managers may purchase necessary accessories as needed, in accordance with Department purchasing procedures and the provisions of this directive. Issued holsters and necessary accessories will be furnished to Agents for use with issued weapons; personally owned holsters and accessories for issued weapons are prohibited. In order to meet unique and specific operational needs and with due consideration for safety, managers may authorize use of alternate holsters and accessories that fully comply with this directive's provisions. Agents must demonstrate proficiency with any authorized holster or accessory prior to carriage or use.

1. Holster Requirements. Authorized holsters must be weapon-specific, cover the trigger guard, allow one handed drawing and re-holstering by the user, and secure the handgun with at least 1 retention device that blocks access or exerts pressure (for example, retention screws or thumb breaks) for holsters where the muzzle does not extend beyond the holster's bottom, or multiple retention devices for holsters where the muzzle does extend beyond the holster's bottom.

2. Optical Devices. Issued optical devices may be used on assigned carbines and issued shotguns, provided that the weapon's iron sights are immediately available to the shooter and that the Agent is not required to remove the optical device or reinstall the

standard sights to transition between optical and iron sights. Once zeroed in, the carbine's front sight must not require additional attention or adjustment by the Agent.

D. **Routine Maintenance of Weapons, Holsters, and Accessories.** Agents are responsible for keeping authorized weapons, holsters, and accessories clean and in operating condition at all times. Agents may only disassemble weapons, holsters and accessories to the extent recommended by the manufacturer for end-users.

E. **Inspections.** Firearms, holsters, and accessories are subject to inspection by an instructor or armorer to ensure they are of proper design and in good repair at any time under order from managers or supervisors, or at the request of an Agent.

1. Firearms. An instructor or armorer will perform a functions check of all authorized firearms and examine all authorized holsters and accessories to ensure that they are in sound working order prior to range qualification. Armorers will annually perform a scheduled full inspection of the mechanical operability of all issued firearms. Firearms that fail a functions check or full inspection will be reported to supervisors before close of business on the day of discovery.

2. Less-Than-Lethal Devices. OC spray and tactical batons shall be annually inspected by a Control Tactics Instructor; if an OC canister is found to weigh less than its net weight or has exceeded its expiration date, it shall be replaced. Also, OC spray and tactical batons shall be replaced if they are found to be inoperable or damaged in any way.

F. **Modification and Repairs.** Modifications or repairs to any authorized weapon, holster or accessory can only be performed by an armorer, the item's manufacturer, or a facility certified by the manufacturer for the type of modification or repair that is required, and only parts made by the manufacturer or to their specifications will be used. Any modification made must be approved and documented by a manager, shall not affect any part of a weapon's internal mechanical operation, and must remain within the manufacturer's specifications. Weapons other than firearms removed for modification or repair may be replaced with an identical item as long as the Agent has demonstrated current proficiency with their original issued item. Upon receipt, Agents are required to demonstrate proficiency with any authorized weapon, holster or accessory that has been modified or repaired prior to carriage or use.

G. **Procurement.** Managers may submit prospective weapons needs through their chain of command for procurement. Used, excess, abandoned, or forfeited weapons must be one of the models (without modification) authorized for use as described in this directive; are in new or like-new condition; and have been inspected by a factory-trained and certified armorer. For ammunition, managers may authorize reasonable purchases to ensure that an adequate supply of ammunition is available at all times for training and duty use.

H. **Accountable Property.** All weapons are accountable property and will be managed in accordance with applicable DOC policies. Weapons that are not issued to a specific Agent must be assigned to a manager. Assignees are responsible for the care, custody and control of assigned property, including compliance with inventory and property management requirements.

VII. **Responsibilities.** In order to oversee and administer policies and training for the effective and responsible use of force, the following roles are established:

A. **Director for Security.** To exercise general oversight for this directive, managers will provide the Director for Security an annual report which documents implementation and compliance.

B. **Special Agent Program Manager.** The SAPM provides technical oversight for all law enforcement powers exercised under OSY policy authority and for all lawful orders issued under the authority of the United States, to specifically include the authority to use force and bear weapons. Managers must promptly inform the SAPM whenever they have information regarding

abuse of authority or misuse of a weapon involving an Agent, and shall consult with the SAPM about weapon procurements prior to disbursement of US Government funds.

C. **Managers and Supervisors.** Managers and supervisors are responsible for implementing this policy and ensuring that every Agent under their command is in compliance. Supervisors must ensure that all Agents under their command authorized to use force comply with training requirements and demonstrate proficiency with authorized weapons. Supervisors are also responsible for ensuring the DOC Hearing Conservation Program is effectively implemented.

   1. Policy Coordinators. Managers in charge of operating units may designate one or more policy coordinators responsible for assisting them in this directive's implementation and documenting compliance as required by this directive.

D. **Instructors and Armorers.** Managers will appoint qualified Agents to serve as Use of Force, Basic Tactics, Control Tactics, and Firearms Instructors, who must graduate from the corresponding FLETC instructor training program and maintain certification in accordance with any FLETC guidelines.

   1. Instructors. Instructors will schedule sessions; provide safe, effective, and documented training; evaluate Agent proficiency, and identify and correct any deficiencies; and make recommendations regarding equipment needs.

   2. Armorers. Managers may also appoint Agents to serve as armorers, who must successfully complete corresponding training provided by the weapon manufacturer (or their authorized representative) for issued weapons, and maintain certification in accordance with any manufacturer recommendations. Armorers will ensure issued firearms are within manufacturer operating specifications.

   3. Policy coordinators may also serve as instructors and/or armorers.

E. **Agents.** Upon initial appointment and thereafter on an annual basis, each Agent will be instructed in and issued a copy of this directive, and must sign a certification acknowledging that they fully understand and agree to comply with its contents.

SPECIAL AGENT DIRECTIVE
APPENDIX 1
ATTACHMENT I

Authorized Qualification Courses of Fire

Handgun: USMS Primary Handgun Qualification, 2/22/15

Handgun: USMS Secondary Handgun Qualification, 2/22/15 (for personally-owned handguns carried when subject to availability or immediate recall)

Shotgun: USMS Shotgun Qualification, 2/22/15

Carbine: USMS AR-15 SMG Qualification, 2/22/15

Authorized Firearms for Issue

Glock M32 .357SIG handgun

Glock M19 9MM handgun

Glock M43 9MM handgun

Wilson Combat Remington 870 12GA shotgun

Land Warfare Resources Corporation 6.8SPC Personal Security Detail carbine

Authorized Personally Owned Handguns

Any publically available double action revolver or semi-automatic pistol in 9MM through .45ACP caliber, excluding any single action handguns, or handguns with barrels exceeding six inches in length

Authorized Ammunition

Commercially manufactured ammunition in 9MM through .45ACP caliber for handguns, 6.8SPC caliber for carbines, or 12GA slug and buckshot for shotguns that has been favorably evaluated by the FBI Firearms Training Unit

Authorized Less-Than-Lethal Devices

SABRE Red Aerosol Oleoresin Capsicum Stream Spray (1.33% Major Capsaicinoids/10% OC/2,000,000,000 SHU)

ASP Friction Loc Baton