~~FOR OFFICIAL USE ONLY /~~
~~ATTORNEY-CLIENT PRIVILEGE~~

OFFICE OF INSPECTOR GENERAL

I&A Identified Threats prior to January 6, 2021, but Did Not Issue Any Intelligence Products before the U.S. Capitol Breach (REDACTED)

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

MEMORANDUM FOR: John Cohen
Senior Official Performing the Duties of the Under Secretary for Intelligence and Analysis
Office of Intelligence and Analysis

FROM: Joseph V. Cuffari, Ph.D.
Inspector General

JOSEPH V CUFFARI
Digitally signed by JOSEPH V CUFFARI
Date: 2022.03.04 16:46:39 -05'00'

SUBJECT: *I&A Identified Threats prior to January 6, 2021, but Did Not Issue Any Intelligence Products before the U.S. Capitol Breach REDACTED*

Attached for your information is our final report, *I&A Identified Threats prior to January 6, 2021, but Did Not Issue Any Intelligence Products before the U.S. Capitol Breach.* We incorporated the formal comments from the Office of Intelligence and Analysis (I&A) in the final report.

The report contains five recommendations to ensure that I&A is better equipped to respond to similar events in the future. Your office concurred with all five recommendations. Based on information provided in your response to the draft report, we consider the recommendations open and resolved. Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may close the recommendations. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions. Please send your response or closure request to OIGISPFollowup@oig.dhs.gov.

Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our report to congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post a redacted version of the report on our website.

Please call me with any questions, or your staff may contact Thomas Kait, Deputy Inspector General for Inspections and Evaluations, at (202) 981-6000.

Attachment

DHS OIG HIGHLIGHTS

I&A Identified Threats prior to January 6, 2021, but Did Not Issue Any Intelligence Products before the U.S. Capitol Breach

March 4, 2022

Why We Did This Evaluation

We initiated this review to determine the actions of Department of Homeland Security's Office of Intelligence & Analysis (I&A) relating to the events at the U.S. Capitol on January 6, 2021.

What We Recommend

We made five recommendations to ensure that I&A is better equipped to respond to similar events in the future.

For Further Information:
Contact our Office of Public Affairs at (202) 981-6000, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov

What We Found

I&A identified specific threat information related to the events on January 6, 2021, but did not issue any intelligence products about these threats until January 8, 2021. Open source collectors in I&A's Current and Emerging Threats Center collected open source threat information but did not produce any actionable information. This resulted from inexperienced open source collectors who received inadequate training and who did not fully consider I&A Guidelines for reporting threat information. Collectors also described hesitancy following scrutiny of I&A's reporting in response to civil unrest in the summer of 2020. Although an open source collector submitted one product for review on January 5, 2021, I&A did not distribute the product until 2 days after the events at the U.S. Capitol. Additionally, I&A's Counterterrorism Mission Center (CTMC) identified indicators that the January 6, 2021 events might turn violent but did not issue an intelligence product outside I&A, even though it had done so for other events. Instead, CTMC identified these threat indicators for an internal I&A leadership briefing, only. Finally, the Field Operations Division (FOD) considered issuing intelligence products on at least three occasions prior to January 6, 2021, but FOD did not disseminate any such products ultimately. It is unclear why FOD failed to disseminate these products.

I&A did email threat information to its local partners in the Washington, D.C. area on several occasions before the events at the U.S. Capitol. However, this information was not as widely disseminated as I&A's typical intelligence products. As a result, I&A was unable to provide its many state, local, and Federal partners with timely, actionable, and predictive intelligence.

I&A Response

I&A concurred with all five recommendations. We consider them resolved and open.

Table of Contents

Background 3

Results of Evaluation 8

OSCO Collected Specific Threat Information about January 6 Events, but Did Not Distribute Any Products until after the U.S. Capitol Breach 9

CTMC Identified Indicators of Potential Violence Regarding January 6, but Did Not Disseminate an Intelligence Product 24

FOD Members Considered Issuing Intelligence Products about January 6 Events, but Did Not Submit Any for Publication 27

I&A Shared Limited Threat Information about January 6 Events with State and Local Partners 28

Recommendations 30

Appendixes

Appendix A: Objective, Scope, and Methodology 35
Appendix B: I&A Comments to the Draft Report 37
Appendix C: Organizational Chart of Relevant I&A Offices 43
Appendix D: Appendix E 44
Appendix E: I&A Timeline Related to January 6 Events 47
Appendix F: Appendix E 49
Appendix G: Appendix F 50

Abbreviations

CETC	Current and Emerging Threats Center
CTMC	Counterterrorism Mission Center
FBI	Federal Bureau of Investigation
FIR	Field Intelligence Report
FOD	Field Operations Division
HSIN	Homeland Security Information Network
I&A	Office of Intelligence and Analysis
IC	Intelligence Community
IIR	Intelligence Information Report
ILD	Intelligence Law Division
IOO	Intelligence Oversight Officer

NTIC	National Capital Region Threat Intelligence Consortium
OGC	Office of General Counsel
OSCO	Open Source Collection Operations
OSIR	Open Source Intelligence Report
RFI	Request for Information

Background

On January 6, 2021, thousands of individuals gathered in Washington, D.C., to protest a Joint Session of Congress to certify results of the Electoral College vote. During the protests, rioters attacked law enforcement, breached barricades, and broke into the U.S. Capitol building, leading to multiple fatalities and the evacuation of Vice President Mike Pence, Members of Congress, and congressional staff. Before January 6, there were at least two instances of violence during Washington, D.C. protests related to the 2020 U.S. Presidential election, resulting in several arrests for assault, possession of dangerous weapons, and inciting violence.[1] Plans for another demonstration during the certification of the Electoral College vote were in place weeks in advance.[2]

After January 6, we initiated this review to evaluate the responsibility of the Department of Homeland Security's Office of Intelligence and Analysis (I&A) for providing intelligence to state and local officials in advance of the events at the U.S. Capitol.[3] We also reviewed whether I&A warned law enforcement about specific threats before the January 6 events.[4]

I&A's Responsibility for Providing Information to State and Local Partners

I&A's mission is to equip the Department of Homeland Security and its partners with timely intelligence and information needed to keep the homeland safe, secure, and resilient. I&A is a member of the U.S. Intelligence

[1] The events occurred on November 14, 2020, and December 12, 2020. For the November 14, 2020 instance, see *Arrests Made in an Aggravated Assault Offense: 1700 Block of I Street, Northwest*, Metropolitan Police Department (Nov. 15, 2020). https://mpdc.dc.gov/release/arrests-made-aggravated-assault-offense-1700-block-i-street-northwest. For the December 12, 2020 instance, see *Additional Arrest Made and Suspects Sought in an Assault with a Dangerous Weapon (Knife) Offense: 500 Block of 11th Street, Northwest* (Dec. 14, 2020). https://mpdc.dc.gov/release/additional-arrest-made-and-suspects-sought-assault-dangerous-weapon-knife-offense-500-block.

[2] See for example, Marrisa Lang, *Trump supporters plan D.C. rally on day Congress certifies election results*, The Washington Post (Dec. 22, 2020). https://www.washingtonpost.com/local/dc-trump-rally-january-6-protests/2020/12/22/1c94ab7a-447a-11eb-a277-49a6d1f9dff1_story.html.

[3] This review is one of three initiated by DHS Office of Inspector General relating to January 6 events; the two other reviews pertain to DHS law enforcement agencies' planning and response efforts. The OIGs for the Departments of Defense, Interior, and Justice also have initiated reviews of their respective agencies' activities relating to January 6 events.

[4] This report defines "January 6 events" as any event, activity, or gathering, whether formal or informal, permitted or unpermitted, taking place in Washington, D.C., related to the January 6, 2021 certification of Electoral College votes by the U.S. Congress. We used this definition when asking I&A employees about intelligence preceding the events at the U.S. Capitol.

Community (IC)[5] and is authorized to access, receive, and analyze law enforcement information, intelligence information, and other information from Federal, state, and local government agencies, and private sector entities, and to disseminate such information to those partners.[6] I&A is the only IC member statutorily tasked with providing intelligence to state, local, and other non-Federal officials.[7]

I&A's intelligence products are governed by IC-specific laws and directives and I&A internal standards. Under Executive Order 12333, I&A is restricted to collecting overtly or through publicly available information,[8] and may analyze and disseminate information and intelligence to its partners to support its national and departmental missions.[9] According to *I&A's Intelligence Oversight Program and Guidelines* (I&A Guidelines),[10] national missions are those that protect the United States' national interests from foreign security threats, while departmental missions assist DHS or other Federal, state, local, or private sector partners in measures regarding threats to homeland security. Specifically, departmental missions include domestic terrorism, critical infrastructure and key resources, and efforts that "support … any … departmental officials, offices, or elements in the execution of their lawful missions."[11]

Relevant I&A Components for January 6 Events

I&A is led by the Under Secretary for Intelligence and Analysis and Principal Deputy Under Secretary. I&A's Intelligence Enterprise Operations is led by a Deputy Under Secretary, who oversees eight offices, including five mission centers that focus on different threat areas. I&A's Intelligence Enterprise Readiness is also led by a Deputy Under Secretary, who oversees areas such as

[5] *See* https://www.intelligence.gov/how-the-ic-works.
[6] 6 United States Code (U.S.C.) § 121(d)(1) and 6 U.S.C. § 121(d)(6).
[7] Other IC agencies are also authorized to share information, including threat-related information, with non-Federal partners.
[8] Overt collection is defined as collection that is openly acknowledged by or readily attributable to the U.S. Government or that would be acknowledged in response to an express inquiry. Publicly available information is defined as information that has been published or broadcast for public consumption, is available on request to the public, is accessible online or otherwise to the public, is available to the public by subscription or purchase, could be seen or heard by any casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any event open to the public.
[9] Executive Order 12333, as amended.
[10] *IA-1000 - Office of Intelligence and Analysis Intelligence Oversight Program and Guidelines,* Jan. 19, 2017 (I&A Guidelines).
[11] *Id.*

training, budget and acquisitions, and intelligence oversight. See Appendix C for an organizational chart of relevant I&A offices.

Our review identified three offices that conducted work related to the January 6 events: the Current and Emerging Threats Center (CETC), Counterterrorism Mission Center (CTMC), and Field Operations Division (FOD).

Current and Emerging Threats Center: CETC provides indication and warning of threats directed against the United States through the collection, analysis, and dissemination of intelligence and information 24 hours a day, 7 days a week. CETC's Open Source Collection Operations branch (OSCO) is the lead for identifying and reporting threats made online via social media and through other sources of publicly available information. OSCO collects threats based on intelligence requirements developed by the IC or Department[12] and provides lead information for law enforcement entities across the country. OSCO's open source collectors often conduct their online searches after receiving requests for information (RFI) or tips about online threats from other I&A offices.

After identifying possible threat information, the I&A Guidelines provide the procedures for collecting, retaining, and disseminating the information. On July 13, 2018, DHS' Associate General Counsel for Intelligence issued a memorandum (DHS Memorandum) that instructs I&A personnel on how to further apply these procedures when collecting and reporting on social media and other publicly available sources.[13] According to the DHS Memorandum, open source collectors may report information in intelligence products when they have a reasonable belief that the information:

- contains true threats or incitement to violence,[14] and not hyperbole;
- provides information that enhances I&A's understanding of known threat actors; or
- includes information that demonstrates a risk of violence during a heightened threat environment.

[12] An intelligence requirement provides instruction for collecting intelligence information, such as searching for a specific national security threat.
[13] *Social Media Statements Referencing Violence Against or Doxxing of DHS Personnel and Facilities,* July 13, 2018 (DHS Memorandum).
[14] A true threat is a statement where the subject means to communicate a serious expression of an intent to commit an act of unlawful violence to a particular individual or group of individuals. Incitement is a statement where the subject means to incite others to engage in violence.

According to the I&A Guidelines, a reasonable belief is defined as a "belief based on facts and circumstances such that a reasonable person would hold that belief." Furthermore:

> A reasonable belief can be experience, training, and knowledge as applied to particular facts and circumstances, and a trained and experienced intelligence professional can hold a reasonable belief that is sufficient to satisfy these criteria when someone lacking such training or experience would not hold such a belief.[15]

When OSCO reasonably believes the information meets the I&A Guidelines for dissemination, it concludes the information meets its "reporting threshold" and drafts an open source intelligence report (OSIR). OSIRs contain raw, unevaluated open source information and do not include analysis.

According to I&A's internal processes, at least one other collector must conduct a peer review of an OSIR before the drafter submits it to a senior collector and ultimately an OSCO supervisor for additional review and approval. The reviewers can provide an opinion on whether the information in the OSIR meets I&A's reporting threshold. When disagreements occur during the review process, the drafter may contact DHS' Office of General Counsel (OGC) Intelligence Law Division (ILD)[16] to receive a legal opinion on whether the information meets the I&A Guidelines.

On October 30, 2020, the I&A Acting Under Secretary issued guidance implementing further review of certain OSIRs before dissemination.[17] According to the guidance, all OSIRs related to the 2020 presidential election had to be reviewed and cleared by both ILD and I&A's Intelligence Oversight Officer (IOO).[18] After all reviews are complete, OSCO publishes the OSIR on the Homeland Security Information Network (HSIN), DHS' official system for sharing unclassified information with state, local, and other partners.

[15] I&A Guidelines.
[16] OGC consists of attorneys and staff working in operational components and headquarters offices, including I&A. ILD advises I&A on legal issues associated with departmental and national intelligence activities.
[17] *Temporary Procedures for Review of Civil Unrest and Certain Election-Related Raw Intelligence*, October 30, 2020.
[18] The IOO ensures OSIRs comply with the I&A Guidelines.

Field Operations Division: FOD is responsible for deploying personnel at fusion centers[19] nationwide and exchanges intelligence information with state and local partners. FOD's Mid-Atlantic Region covers Washington, D.C.; one intelligence officer is posted to the Washington, D.C. fusion center, formally named the National Capital Region Threat Intelligence Consortium (NTIC), and exchanges information with Washington, D.C. law enforcement organizations, including the Washington, D.C. Metropolitan Police Department and the U.S. Capitol Police.

FOD provides OSCO tips relating to online threat information, which FOD might receive from state, local, and other partners. OSCO either produces an OSIR on the information or tells FOD the information does not meet its reporting threshold. In addition, FOD can draft its own intelligence products, including Field Intelligence Reports (FIR) and Intelligence Information Reports (IIR). Similar to OSIRs, FIRs and IIRs are raw intelligence products that record, but do not analyze, the identified information. FIRs meet DHS intelligence requirements and are published via HSIN, while IIRs meet IC intelligence requirements and may be published on HSIN or a classified system depending on their classification.[20]

Counterterrorism Mission Center: CTMC analyzes terrorism-related intelligence and produces analytic intelligence products. For these products, CTMC intelligence analysts may analyze the information recorded in OSIRs, FIRs, IIRs, other products, and open source reporting and make assessments and judgments on the information. CTMC also sends RFIs to OSCO asking collectors to research and consider producing OSIRs on a particular threat or event. After OSCO produces OSIRs on the issue, CTMC may cite them in an analytic intelligence product. CTMC publishes unclassified products on HSIN.

Prior Reporting on Protest Activity

During the summer of 2020, I&A produced open source intelligence reporting in response to civil unrest in Portland, Oregon.[21] However, I&A faced criticism

[19] Fusion centers "serve as focal points in states and major urban areas for the receipt, analysis, gathering and sharing of threat-related information between State, Local, Tribal and Territorial (SLTT), federal and private sector partners." https://www.dhs.gov/fusion-centers.
[20] DHS intelligence requirements may not align with IC intelligence requirements. For example, information about domestic terrorism or a threat to U.S. critical infrastructure may meet a DHS intelligence requirement but not an IC intelligence requirement. In this instance, FOD could write an FIR about the information, but not an IIR.
[21] For other OIG work related to DHS' response to civil unrest in Portland, Oregon, see *Management Alert – FPS Did Not Properly Designate DHS Employees Deployed to Protect Federal Properties under 40 U.S.C. § 1315(b)(1),* OIG-21-05, Nov. 2, 2020, and *DHS Had Authority to*

for compiling intelligence on American journalists reporting on the unrest as well as on non-violent protesters.[22] Although this review did not assess the appropriateness of I&A's reporting on Portland in the summer of 2020, these circumstances provide important context for I&A's decisions and actions leading to the January 6 events.

Results of Evaluation

In the weeks before the events at the U.S. Capitol, I&A identified specific open source threat information related to January 6 but did not issue any intelligence products about these threats until January 8.[23] Within OSCO, staff collected open source threat information but did not produce any actionable information. This resulted, in part, from inexperienced collectors who received inadequate training and did not fully consider I&A Guidelines for reporting threat information. Collectors also described hesitancy to report information following scrutiny of I&A's actions in Portland, Oregon, in the summer of 2020. Although an OSCO collector submitted one product for review on January 5 regarding possible violence, I&A did not distribute the product until 2 days after the events at the U.S. Capitol. Additionally, CTMC identified indicators that the January 6 events might turn violent but did not issue an intelligence product outside I&A, even though it had done so for other events. Instead, CTMC identified these threat indicators for an internal I&A leadership briefing, only. Finally, FOD considered issuing intelligence products on at least three occasions prior to January 6 but ultimately did not disseminate any. It is unclear why FOD chose not to move forward with issuing an intelligence product.

Although I&A did not disseminate any related intelligence products prior to January 6, it emailed threat information to its local partners in the Washington, D.C. area on several occasions. However, this information was emailed to select partners and was not as widely disseminated as I&A's typical

Deploy Federal Law Enforcement Officers to Protect Federal Facilities in Portland, Oregon, but Should Ensure Better Planning and Execution in Future Cross-Component Activities, OIG-21-31, Apr. 16, 2021.

[22] An August 3, 2020 letter from the Permanent Select Committee on Intelligence, U.S. House of Representatives, to DHS Acting Secretary Chad Wolf and Acting Under Secretary for Intelligence and Analysis Brian Murphy, states, "[a]ccording to press reports, I&A engaged in intelligence collection and reporting on journalists and non-violent protestors." https://intelligence.house.gov/uploadedfiles/20200803_chm_letter_to_murphy_wolf_re_civil_liberties.pdf.

[23] See Appendix E for a timeline about I&A's work related to January 6 events between December 21, 2020, and January 8, 2021.

intelligence products. As a result, I&A was unable to provide its many state, local, and Federal partners with timely, actionable, and predictive intelligence.

OSCO Collected Specific Threat Information about January 6 Events, but Did Not Distribute Any Products until after the U.S. Capitol Breach

OSCO collectors received an RFI and open source tips about January 6 events, and identified specific threats about storming the U.S. Capitol and targeting law enforcement. However, the collectors did not produce any actionable intelligence products because they received inadequate training and did not fully consider the I&A Guidelines for reporting threat information. They also described hesitancy to report information following scrutiny of I&A's actions in Portland, Oregon. Although an OSCO collector submitted one product for review before January 6, I&A did not distribute the product until January 8.

OSCO Received an Urgent RFI Related to the January 6 Events and Began Tracking Relevant Threats

On December 29, 2020, CTMC sent OSCO an RFI for threat information regarding January 6 events, such as:

- Online calls by event organizers to bring weapons to lawful protests or counter protests;
- Increase in lawful protesters or counter protesters in Washington, [D.C.] carrying, brandishing, or using more lethal weapons, such as firearms or edged weapons;
- Specific directed threats of violence towards primary protest organizers or prominent ideological adversaries or figures associated with an ideological movement; [and]
- Violent extremists posing a threat to individuals to include [law enforcement] and government officials, who hold opposing views prior to scheduled events.

The RFI listed the U.S. Capitol Police, the United States Secret Service, and other Federal, state, and local partners as intended recipients of the information. The CTMC intelligence analyst who drafted the RFI said he expected OSCO to post OSIRs about January 6 threats on HSIN, where the intended recipients could access them.

In the email transmitting the RFI, CTMC informed OSCO that this was an urgent request. Within the RFI itself, CTMC explained the information would

no longer be of any value by January 7 because I&A must inform Federal, state, and local partners about the threats "so contingency plans can be made for any planned events." CTMC also warned that threat actors might delete information online as the date got closer to January 6 to evade law enforcement detection.

After receiving the RFI, seven OSCO collectors researched possible threats to January 6 events and recorded their findings in a document tracking threats responsive to CTMC's request. Between December 29, 2020, and January 3, 2021, five of these collectors identified comments referencing using weapons and targeting law enforcement and the U.S. Capitol building. They also noted some individuals claimed they would sacrifice themselves in the ensuing violence. Table 1 provides excerpts from OSCO's document tracking January 6 threats in response to the RFI. See Appendix D for all January 6 threats documented by these five collectors.

Table 1. Excerpts from OSCO Document Tracking January 6 Threats

Date OSCO Identified Threat	Description of Threat by OSCO Collector
December 29	An individual suggested [redacted] in Washington, D.C.
December 30	An individual posted, [redacted]
December 30	An individual claimed there would not be enough law enforcement officers to stop the number of armed people arriving in the area.
January 2	Posts referenced the [redacted] of Congress.
January 2	Individuals shared images of the U.S. Capitol building and its [redacted]
January 2	An individual stated, [redacted]
January 2	One post stated, [redacted]
January 2	Posts from approximately 12 individuals said they [redacted]

Source: DHS OIG analysis of I&A information

We did not locate any evidence that the five collectors drafted an OSIR about any of the threats recorded in their document.

OSCO Received Open Source Tips about January 6 Threats from FOD

In addition to the RFI from CTMC, OSCO also received tips about online threats from FOD. However, OSCO did not produce any OSIRs based on FOD's tips about January 6 threats.

On December 21, 2020, FOD shared a tip[24] with OSCO about an individual who threatened to shoot and kill protesters at the upcoming rallies related to the presidential election.[25] According to the tip, as shown in Figure 1, the individual informed members of an online discussion group that he planned to kill at least 50 individuals.

Figure 1. December 21, 2021 Tip from FOD[26]

[redacted]

Source: I&A

Later that day, an OSCO collector told FOD that she could not locate the [redacted], and that OSCO had to [redacted]. However, FOD never responded, and on December 31, 2020, the FOD member acknowledged to a colleague that the email from OSCO "slipped away" from her. OSCO did not draft an OSIR based on this tip.

On January 5, 2021, FOD provided a tip to OSCO about a social media user calling for people to come to Washington, D.C., to counter the protests and stated, [redacted] Following the tip, OSCO researched the social media account and informed FOD it was "unable to find any derogatory information."

On January 6 at 11:29 a.m., FOD provided a tip about a social media user claiming the Proud Boys planned to shut down the Washington, D.C. water system, as shown in Figure 2. At 2:53 p.m., shortly after the U.S. Capitol

[24] FOD received the tip from the SITE Intelligence Group, a non-governmental organization that tracks online activity of terrorist and violent extremist groups.
[25] FOD also considered drafting an intelligence product about this threat, as discussed later in this report.
[26] Figure 1 and other figures in this report redact certain information to protect online identities or remove explicit language.
[27] The Proud Boys group was involved in the two prior instances of violence during protests related to the 2020 U.S. Presidential election in Washington, D.C., on November 14, 2020, and December 12, 2020.

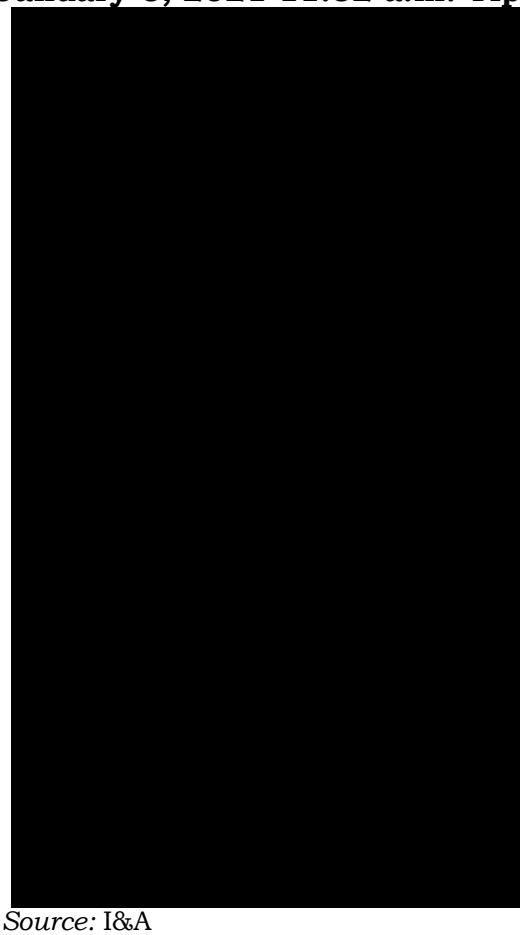
breach, OSCO notified FOD that this information did not meet its reporting threshold.

Figure 2. January 6, 2021 11:29 a.m. Tip from FOD

Source: I&A

On January 6 at 11:32 a.m., FOD provided two additional tips about threats to Washington, D.C. Both tips referenced [redacted] as shown in Figure 3.

Figure 3. January 6, 2021 11:32 a.m. Tip from FOD



Source: I&A

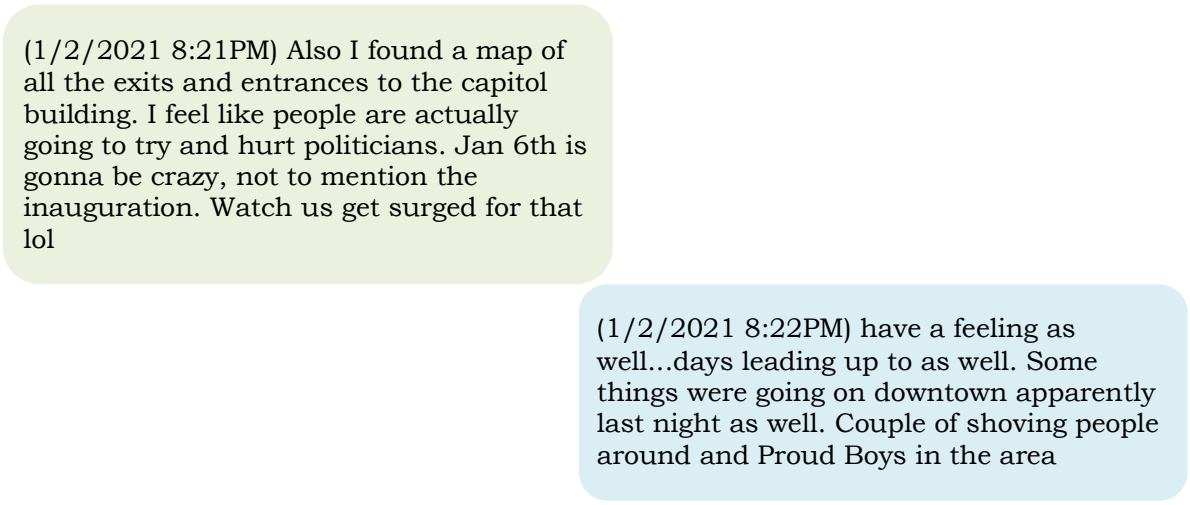
We found no evidence that OSCO informed FOD whether these two tips met I&A's reporting thresholds.

Collectors Discussed January 6 Threats and Washington, D.C. Safety Concerns with Each Other

On several occasions leading up to January 6, collectors messaged each other about the threats they discovered online. These threats included individuals storming the U.S. Capitol, targeting politicians and law enforcement, and sacrificing their lives while conducting violence. Additionally, collectors said they were concerned about safety in Washington, D.C. on January 6.

On January 2, 2021, after a collector learned that individuals online were sharing a map of the U.S. Capitol building, he messaged his colleague saying he thought people would "try and hurt politicians." In response, the colleague agreed with this assessment. The two OSCO members also noted the possibility of I&A ordering an employee "surge" to respond to the escalating threats[28] but did not discuss the possibility of issuing an intelligence product.

Figure 4. Messages between OSCO Collectors January 2, 2021 8:21 – 8:22 p.m.

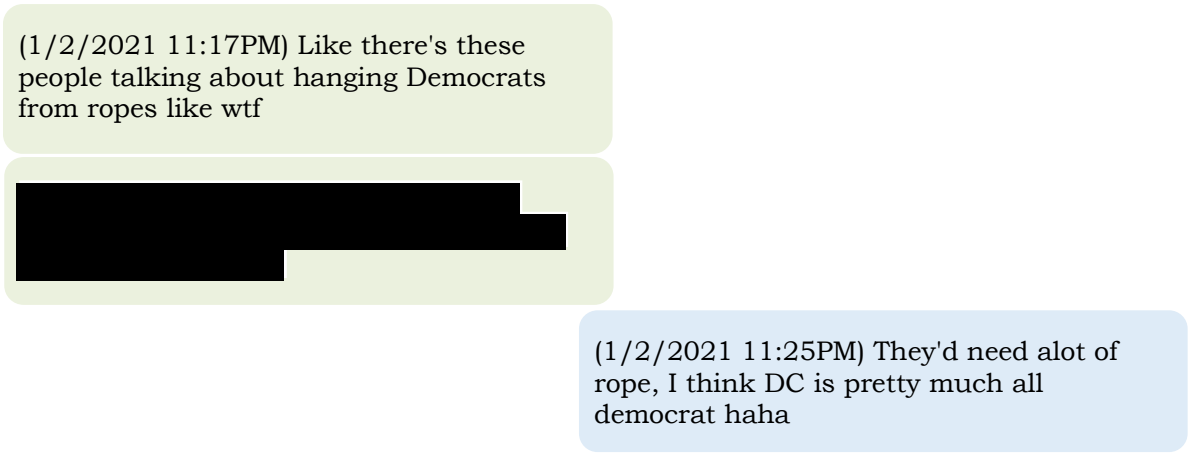


Source: DHS

Also on January 2, 2021, two collectors discussed online comments threatening to hang Democrats in Washington, D.C. but did not think the comments met the reporting threshold.

[28] During a "surge," I&A asks OSCO collectors to work extra hours to respond to crises.

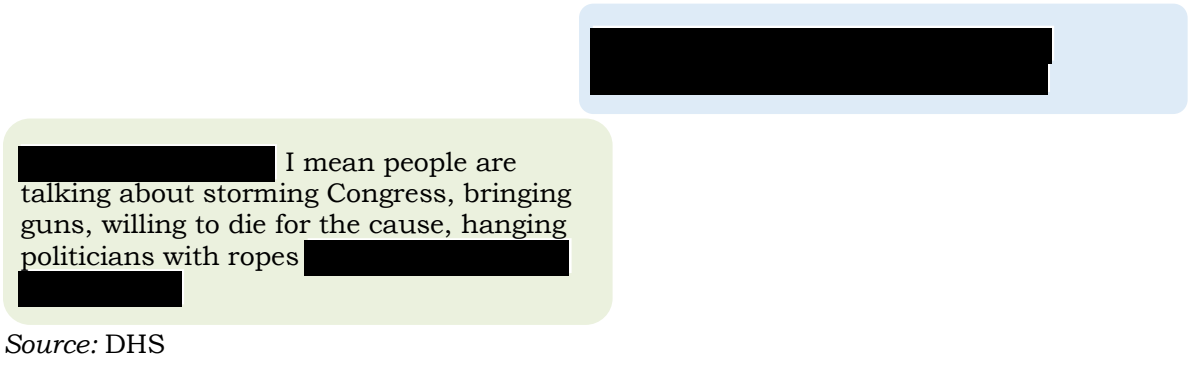
Figure 5. Messages between OSCO Collectors
January 2, 2021 11:17 – 11:25 p.m.



Source: DHS

The following morning, these collectors noted individuals were discussing hanging politicians, storming Congress, and sacrificing their lives, but the collectors said the information still did not meet the reporting threshold. They did not draft any related OSIRs.

Figure 6. Messages between OSCO Collectors
January 3, 2021 2:53 a.m.



Source: DHS

These two collectors continued to discuss their view that the threats were unlikely. Although one collector suggested he "could be proven wrong," they did not consider issuing OSIRs about the possibility of these threats occurring.

In other instances, collectors expressed nervousness about the information they were uncovering and concern about each other's safety in the Washington,

D.C. area. One OSCO member told us that they "were clearly concerned" and told each other to "stay safe" throughout the week. Others told each other they would stay home on January 6 to avoid potential violence.

Additionally, on January 4, 2021, an open source collector learned a group of individuals already arrived in Washington, D.C. and were posting social media content that sounded "like they are going to battle." Following this, the open source collector and a colleague both said they were "nervous" about how January 6 events would unfold in the area. Yet, these collectors did not draft any intelligence products reflecting possible safety concerns in the area.

OSCO Did Not Issue Any OSIRs about January 6 Threats before the U.S. Capitol Attack

Despite encountering threats while conducting research for CTMC's RFI, receiving online tips from FOD, and expressing concerns about the information internally, OSCO did not issue any OSIRs about this information to inform its partners of possible threats for January 6. We identified multiple reasons why OSCO collectors did not publish OSIRs about these threats before the U.S. Capitol attack. Specifically, inexperienced collectors received inadequate training related to open source collection, did not fully consider the I&A Guidelines for reporting threat information, and were hesitant to report information following scrutiny of I&A's actions in Portland, Oregon, in the summer of 2020.

Inexperienced Open Source Collectors Received Inadequate Training

OSCO rapidly hired inexperienced open source collectors in the months leading up to January 6, 2021. When OSCO switched to a 24 hours per day schedule in the summer of 2019, with shift changes at 5 a.m., 1 p.m., and 9 p.m., many collectors left. OSCO began hiring new collectors, mostly at entry level positions, with many not having Federal government or intelligence experience. As of January 6, 2021, 16 out of 21 collectors had less than 1 year of experience, and some of these new collectors said they did not receive adequate training to help determine when threat information should be reported.

Following the hiring process, I&A did not offer any training courses designed for OSCO collectors. Instead, collectors trained informally by working alongside colleagues with more experience. Several collectors described this approach as insufficient, with one collector calling it "haphazard" and "not organized," and another saying it should not have been considered training at all. This informal training was even more limited during the COVID-19 pandemic, when new collectors could only come to the office part time and had

fewer opportunities to work with their colleagues during shifts. I&A also instructed new collectors to take online training courses, but these courses were not developed specifically for I&A collectors conducting open source intelligence.

In September 2020, following criticism by Congress and in the media about I&A's open source intelligence reporting in response to civil unrest in Portland, Oregon, I&A developed a formal training course and provided it to all collectors. However, I&A tasked two OSCO members to develop the training on short notice without any input from experienced training instructors. I&A did not receive any assistance from I&A's Intelligence Training Academy, which is specifically tasked with developing and delivering homeland security intelligence training. According to one I&A official, the academy takes approximately 6 months to put a training program together. In contrast, OSCO developed its training course within a few weeks, causing one OSCO member to speculate that I&A developed this course quickly to avoid more criticism of its actions during civil unrest in the summer of 2020, rather than to create an effective training program.

Certain collectors told us they were still unsure about when information should be reported following the more formal training. For example, one collector said the formal training did not define reporting thresholds sufficiently, which caused confusion during the OSIR peer review process. Another collector said the training could have provided better direction to OSCO members. She added that although a training instructor said collectors could contact ILD when they have a question about a reporting threshold, she was also aware that ILD did not operate on a 24 hours per day schedule and may not be available when OSCO members have a question. However, during the election period, ILD expanded its operating hours and remained on call to answer collectors' questions.

I&A leadership expressed concerns the day before the U.S. Capitol breach that experienced instructors were not leading OSCO's training. On January 5, 2021, the Acting Deputy Under Secretary for Intelligence Enterprise Operations wrote to other senior I&A officials, "I don't feel comfortable having CETC continue to be the [primary] leader of this training."

Later in January, I&A leadership identified shortcomings in its open source training curriculum. In a January 25, 2021 memorandum, I&A's two Deputy Under Secretaries described its open source training as "incomplete" and said it "presents risks such as unmet collection needs and deficient collection-related skills." The memorandum identified actions that I&A needed to take to prevent these risks, such as creating standardized qualifications for the

collectors and aligning training to these qualifications. Until this training curriculum is updated, collectors will continue to receive training that does not adequately prepare them to respond to open source threats.

Collectors Did Not Appear to Fully Consider the I&A Guidelines

As described previously, open source collectors may report information from social media and other publicly available sources in intelligence products when they have a reasonable belief that the information:

- contains true threats or incitement to violence, and not hyperbole;
- provides information that enhances understanding of known threat actors; or
- includes information that demonstrates a risk of violence during a heightened threat environment.

When reviewing threats pertaining to January 6 events, the collectors generally concluded that the statements online were hyperbole, and not true threats or incitement, because they thought storming the U.S. Capitol and other threats were unlikely or not possible. After concluding the information was hyperbole, the collectors determined they could not report the information and did not consider whether it met either of the other two criteria for open source intelligence reporting. For example,

- On January 4, an OSCO collector reviewed [redacted] and assessed that the information appeared to contain threats to law enforcement officers. One [redacted] specifically referenced [redacted] and armed individuals [redacted]:

Figure 7. January 4 Screenshot of Online Forum

[redacted]

Source: DHS

The collector and others on her shift initially agreed that this information met I&A's reporting threshold. However, the collector was nearing the end of her shift and did not think she had time to draft an OSIR. Instead, she emailed the screenshots to collectors on the next two shifts so they could consider disseminating an OSIR about these threats. The next shifts' collectors decided the information was hyperbole and recommended against dissemination. One collector responded, "[s]ome posts either appeared hypothetical, vague, or hyperbolic," while other posts were not "specific enough" to "meet OSIR threshold." After a supervisor also said he did not think the information was reportable, the collector refrained from drafting an OSIR on the threats.

- On January 4, another OSCO collector drafted an OSIR about individuals planning to sacrifice their lives during violence on January 6. The drafter documented one individual [redacted] The drafter noted that another individual suggested storming the U.S. House of Representatives chamber in the U.S. Capitol and mentioned grievances about police in Washington, D.C. Ultimately, he and another collector decided the threats were hyperbole and did not submit the OSIR for review.

In neither of the two examples, nor in other reviewed documentation, did we find evidence that collectors considered whether the information met either of the other two reporting criteria.

Overall, open source collectors explained to us that they did not think storming the U.S. Capitol was possible, and, therefore, they dismissed this specific type of threat as hyperbole. For example, two collectors said this type of threat online was common and doubted the legitimacy of the threat prior to January 6. Another collector said OSCO did not think anyone would be able to breach the U.S. Capitol, but "unfortunately," OSCO was "wrong." As a result, despite several collectors documenting threats to storm the U.S. Capitol building, they concluded that they could not report it to I&A's state and local partners.

The I&A Guidelines allow open source collectors to report information that enhances I&A's understanding of known threat actors, even if the information does not include true threats or incitement. ILD explained to us that a known threat actor is a group that has been the subject of previous intelligence, and I&A could conduct more expansive collection about information relating to these groups. One collector did identify online posts about January 6 events by the Proud Boys, a known threat actor. However, a colleague reviewing the information said, [redacted] The colleague subsequently said, [redacted] without considering whether the information enhanced I&A's understanding of known threat actors.

DHS Memorandum

- CONTAINS TRUE THREATS OR INCITEMENT TO VIOLENCE, AND NOT HYPERBOLE;
- PROVIDES INFORMATION THAT ENHANCES UNDERSTANDING OF KNOWN THREAT ACTORS; OR
- INCLUDES INFORMATION THAT DEMONSTRATES A RISK OF VIOLENCE DURING A HEIGHTENED THREAT ENVIRONMENT

I&A may also report information about a risk of violence during a heightened threat environment, even if the information does not include true threats or incitement. Prior to January 6, other I&A offices issued intelligence products warning of a heightened threat environment because of domestic extremist threats.[29] However, I&A's Acting Deputy Under Secretary informed us that OSCO was not operating under a heightened threat environment at the time. According to the Acting Deputy Under Secretary, operating under a heightened threat environment would have lowered the reporting threshold to make it easier to disseminate information at a time when attacks may occur with minimal or no advanced warning.

Instead, OSCO collectors thought their reporting threshold was particularly high leading up to January 6. For example, one collector messaged a colleague on January 3 saying, "there are threats," but "our threshold is just very high now." Another collector told us the reporting threshold for domestic terrorism threats was so high that it made any open source reporting unfeasible, while another said to us that OSCO had a very high threshold at the time and the

[29] According to the March 3, 2021 testimony by the Acting I&A Under Secretary, I&A issued more than 15 warnings to its Federal, state, and local partners about the heightened threat from domestic extremists before January 6.

collectors were nervous to report anything. We found no evidence that the collectors considered their own agency's warnings about the heightened threat environment when contemplating whether threats met I&A's reporting thresholds.

Scrutiny of OSCO Collectors' Work during Prior Civil Unrest Affected Their Approach to Reporting Threats for January 6

Following criticism about I&A's intelligence activities in response to civil unrest during the summer of 2020 in Portland, Oregon, I&A leadership launched a review of OSIRs that collectors published during the unrest. The CETC Director, who oversees OSCO, reviewed the OSIRs to determine whether products failed to meet the I&A Guidelines. On August 7, 2020, the CETC Director released a memo outlining his review of 366 OSIRs published by OSCO between May 25, 2020, and August 4, 2020. In the memo, the CETC Director concluded that 22 did not meet reporting thresholds in accordance with the I&A Guidelines. On September 25, 2020, the CETC Director determined one additional OSIR did not meet reporting thresholds after an I&A internal auditor raised concerns about other OSIRs published during the summer of 2020. In total, CETC recalled 23 OSIRs.

Within OSCO, 22 of 24 members told us their approach to reporting for January 6 events was affected by the scrutiny they received following the summer of 2020. In some instances, OSCO personnel described a "pendulum swing." They explained that they thought almost anything was reportable during the Portland protests, but they were hesitant or fearful to report information related to January 6 events. One collector said people were afraid to do their jobs because of the fear of being reprimanded by I&A leadership and concerns about congressional scrutiny. Another explained there was a "chilling effect" on their approach to reporting following the summer of 2020.

OSCO staff shared with each other their hesitancy to collect information on January 6 events because of the scrutiny they previously received. On December 24, 2020, two collectors discussed protestors planning to bring weapons to Washington, D.C. on January 6. The collectors mentioned a third collector's concern for sharing this information within I&A because of [redacted] to which the other collector responded:

[redacted]

[redacted]

When we asked the Acting Deputy Under Secretary about the change in CETC's approach to reporting, she noted that there was different leadership for the summer of 2020 compared to January 6, 2021.[30] She said the prior leadership pushed collectors to report on anything related to violence, including potential threats or tactics and techniques used by individuals that may be associated with violence. In contrast, the new leadership encouraged collectors to issue intelligence reports on threats only when they were confident the threats were real. The Acting Deputy Under Secretary said this change in direction went too far and caused collectors to institute a very high threshold for reporting information.

A Collector Submitted a Draft OSIR on January 5, but OSCO Leadership Failed to Complete the Review Process before the U.S. Capitol Breach

Although OSCO did not disseminate an OSIR prior to the U.S. Capitol breach on January 6, we found an instance in which it did release one product related to that day's events. However, the OSIR was not disseminated until 2 days after the breach, rendering it useless for the purposes of advanced warning. On January 5, an OSCO collector identified a potential threat of violence related to January 6 events and concluded it met I&A Guidelines. Specifically, the open source collector discovered a [redacted] about an individual arriving in the Washington, D.C. area and searching for a location for armed individuals to park their cars. The individual previously posted online that he would arrive in the area [redacted] and he was [redacted] Washington, D.C.

After the collector drafted an OSIR about the threat, another OSCO collector performed the peer review on January 5 and said the information did not meet reporting thresholds because it only contained hyperbolic information. However, at the request of the OSIR drafter, ILD agreed to review the product.

ILD spoke with the OSIR drafter on the phone on January 5, informed the OSIR drafter that the information contained in the OSIR met I&A's reporting guidelines, and summarized this phone call in an email to the drafter, another collector, and OSCO supervisors on January 6 at 12:16 a.m. ILD outlined how the information [redacted]

[30] DHS replaced I&A's Under Secretary on August 1, 2020. In November 2020, I&A hired a new CETC Director and moved the former CETC Director to the role of Deputy Director.

[redacted] According to ILD:

[redacted]

ILD also suggested [redacted]

After ILD cleared the product, OSCO supervisors did not request IOO review and clearance (as required for election-related raw intelligence) until about 15 hours later at 5:22 p.m. on January 6, after the U.S. Capitol breach.[31] We found no evidence that OSCO supervisors took any action regarding the OSIR during the intervening 15 hours, and it is unclear why OSCO waited until after the U.S. Capitol breach to ask the IOO for the review. After receiving OSCO's request for review, the IOO consulted with ILD and other intelligence oversight partners and also provided clearance for the dissemination of the product on January 7.

On January 8, before publishing the product, OSCO once again asked ILD and the IOO to review the product before dissemination. In response, ILD expressed confusion at OSCO's repeated requests to review the product before dissemination. ILD's email states:

[redacted]

[31] Rioters breached the U.S. Capitol building at approximately 2:15 p.m. ET.

[redacted]

Although the OSCO collector drafted the OSIR on January 5, the day before the U.S. Capitol breach, the OSIR was not finalized and disseminated until January 8, 2 days after the breach. Table 2 shows a timeline of the drafting and dissemination process for the OSIR.

Table 2. Timeline of the OSIR Review Process

Date	Actions related to the OSIR review process
January 5 8:59 a.m.	Collector submitted a draft OSIR related to January 6 events for peer review.
January 5 10:27 a.m.	Peer reviewer said the OSIR did not meet I&A's reporting thresholds.
January 5 10:54 a.m.	Collector sent a message to the peer reviewer saying he spoke on the phone with ILD about the draft OSIR and received clearance to disseminate the OSIR.
January 5 2:24 p.m.	Collector emailed ILD to receive a written legal opinion about whether the OSIR met the I&A Guidelines.
January 6 12:16 a.m.	ILD sent an email summarizing why the OSIR likely met the I&A Guidelines and stating it was appropriate to [redacted]
January 6 2:15 p.m.	**Rioters breached the U.S. Capitol building.**
January 6 5:22 p.m.	An OSCO supervisor asked the IOO to review the product.
January 7 2:02 p.m.	The IOO said she consulted with ILD and other intelligence oversight partners and reviewed and cleared the product for dissemination.
January 8 10:57 a.m.	An OSCO supervisor asked ILD and the IOO to review the product again before dissemination.
January 8 11:47 a.m.	ILD informed OSCO that it was [redacted]
January 8	I&A published the OSIR on HSIN.

Source: DHS OIG analysis of I&A information

CTMC Identified Indicators of Potential Violence Regarding January 6, but Did Not Disseminate an Intelligence Product

On several occasions, CTMC has disseminated an intelligence product evaluating the possibility for violence at certain locations, such as during protests. These products ("probable indicator products") include eight indicators that demonstrate a possibility of violence. For example, one indicator is whether individuals call for violent extremists to attend protests, while another indicator is whether there are threats towards either protest organizers or "prominent figures" with ideologically opposed views. The product then describes which indicators are observed, partially observed, or not observed.[32] According to CTMC, identifying multiple observed or partially observed indicators likely suggests the increased probability of violence.

We determined CTMC has published at least three probable indicator products, including one prior to the January 6 events, and posted these products on HSIN to share them with state, local, and other partners. Specifically, on September 5, 2020, I&A disseminated on HSIN a probable indicator product that identified five observed or partially observed indicators of possible protest-related violence in Portland, Oregon.[33]

On January 4, 2021, the Acting Deputy Under Secretary tasked CTMC with analyzing indicators of potential protest-related violence in Washington, D.C. In its analysis, CTMC identified seven observed or partially observed indicators of potential violence associated specifically with the protests planned for January 6. For example, CTMC determined that an indicator about event organizers calling for protesters to bring weapons was observed, and referenced six media articles about the January 6 events. However, this analysis was intended for an internal briefing only and not for a published product. CTMC briefed I&A leadership and the DHS Deputy Secretary on these indicators on the morning of January 6; the product was not disseminated more widely on HSIN or outside DHS in any other manner.

We compared the September 5, 2020 probable indicator product about threats in Portland, which was disseminated on HSIN, to the analysis about possible

[32] CTMC determines indicators are partially observed when it discovers relevant but "vague and non-specific" information.
[33] In addition, CTMC published two probable indicator products after January 6. On January 14, 2021, CTMC published a product about possible protest-related violence in Washington, D.C. leading up to and on Inauguration Day. On February 11, 2021, CTMC published a product about possible violence in the Washington, D.C. area, including violence unrelated to protest activity.

violence on January 6 in Washington, D.C., which was not disseminated. Despite identifying more indicators of possible violence than the product about threats in Portland, CTMC did not similarly disseminate its analysis about January 6 threats. Table 3 describes each of the eight indicators, as well as whether CTMC analysts thought they were observed or not observed in Portland and Washington, D.C.[34]

Table 3. Comparison of Probable Indicators of Escalation of Protest-Related Violence

Probable Indicators of Escalation of Protest-Related Violence	Portland, Oregon Summer 2020	Washington, D.C. January 6, 2021
Online calls by event organizers to bring weapons to lawful protests or counter protests.	Partially Observed	Observed
Increase in lawful protesters or counter protesters carrying, brandishing, or using more lethal weapons, such as firearms or edged weapons.	Partially Observed	Partially Observed
Widespread calls by event organizers for violent extremists to attend lawful protests or counter protests.	Partially Observed	Partially Observed
Specific, directed threats of violence towards primary protest organizers or prominent figures associated with an ideological movement.	Not Observed	Observed
Increase in the frequency of violent clashes occurring between ideologically opposed groups of individuals.	Observed	Partially Observed
Public announcements that prominent figures associated with ideological movements will attend planned protests.	Not Observed	Observed
Violent extremists seeking out and confronting individuals who hold opposing views prior to scheduled events.	Not Observed	Not Observed
Longer lead times between the announcement of protests and the date of the events.	Partially Observed	Observed

Source: DHS OIG analysis of I&A information

[34] In Table 3, observed indicators of possible violence are indicated in red; partially observed indicators of possible violence are indicated in orange; and non-observed indicators of possible violence are indicated in yellow.

We asked the Acting Deputy Under Secretary why the January 6 analysis was not disseminated as the Portland product had been. She said she did not ask CTMC to issue a probable indicator product before the January 6 events because there was not enough time. She explained that she tasked CTMC to conduct this analysis 2 days before the events, and I&A cannot publish a CTMC product within that timeframe. In light of this time constraint, the Acting Deputy Under Secretary said she tasked CTMC with this assignment to ensure it was prepared to brief leadership about the threats, rather than to disseminate a product.

However, as described earlier, CTMC had already submitted an RFI to OSCO for threat information on December 29, 2020, almost a week before the Acting Deputy Under Secretary's tasking. Additionally, CTMC has demonstrated that it can issue products related to indicators of violence within short timeframes. For example, on January 11, a CTMC intelligence analyst informed other CTMC staff that they were tasked with drafting a probable indicator product related to Washington, D.C. and the presidential inauguration. CTMC analysts completed their first draft of the product on January 11, and I&A posted the final product on HSIN on January 14. This product identified seven observed or partially observed indicators of possible protest-related violence in Washington, D.C. leading up to Inauguration Day.

CTMC's ability to issue an intelligence product about January 6 events may have been limited by the absence of OSIRs issued by OSCO on these threats. CTMC's analytic intelligence products often rely on the information in OSIRs or other intelligence reports, rather than media articles.[35] When CTMC sent an RFI for January 6 threat information to OSCO, it expected OSCO to publish OSIRs on these threats. This would have enabled CTMC to cite OSIRs about January 6 threats in an analytic intelligence product.

During our interviews, some I&A employees discussed how products that provide indicators or warnings about upcoming threats can be helpful to state and local officials. One FOD member assigned to the Mid-Atlantic Region reviewed CTMC's indicator analysis prior to January 6 and said this information would have been "incredibly helpful." However, CTMC did not place this analysis in a final product for dissemination to local officials before the U.S. Capitol breach.

[35] CTMC explained that while this is not a requirement, it is considered good intelligence tradecraft for producing analytic intelligence reports.

FOD Members Considered Issuing Intelligence Products about January 6 Events, but Did Not Submit Any for Publication

In addition to submitting tips to OSCO, FOD members in the Mid-Atlantic Region considered issuing intelligence products on at least three occasions about threats to the January 6 events. Despite identifying these threats, FOD members did not submit any intelligence products for publication and were unable to explain to us what happened in each of these three instances.

On December 21, two FOD members assigned to the Mid-Atlantic Region considered issuing two FIRs on possible threat information related to January 6. At 12:26 p.m., a FOD member shared with other FOD staff in the region an online threat about an individual threatening to shoot and kill protesters at upcoming rallies. A supervisor recommended both issuing an FIR and sending a tip to OSCO with the information.[36] At 3:10 p.m., the FOD member informed his supervisor that he and a colleague would write another FIR about threats posted on online forums. According to the FOD member, the online forums discussed bringing unpermitted weapons to Washington, D.C., evading law enforcement detection, and threatening U.S. Congress and politicians. The FOD member asked NTIC to conduct additional research on these threats and planned to add NTIC's feedback to the FIR.

The FOD member informed his supervisor the following day that FOD leadership recently placed a hold on all FIRs. FOD drafts and posts FIRs on unclassified systems. However, FOD leadership became concerned about possible security compromises affecting unclassified systems after the 2020 SolarWinds Orion security breach.[37] As a result, FOD leadership advised that issuing IIRs on a classified system may continue while pausing production of FIRs and IIRs on HSIN.

IIRs must meet IC intelligence requirements, which may not align with the DHS intelligence requirements for FIRs.[38] A FOD member informed his supervisor that a colleague would conduct research to determine whether one of the

[36] As previously noted, FOD sent this tip to OSCO (see Figure 1). OSCO asked a question about the tip, but FOD never responded.
[37] According to DHS' Cybersecurity and Infrastructure Security Agency, "an advanced persistent threat (APT) actor added malicious code to multiple versions of the SolarWinds Orion platform and leveraged it—as well as other techniques—for initial access to enterprise networks of U.S. government agencies, critical infrastructure entities, and private sector organizations." https://www.cisa.gov/sites/default/files/publications/CISA_Insights_SolarWinds-and-AD-M365-Compromise-Risk-Decisions-for-Leaders_0.pdf.
[38] If information meets a DHS intelligence requirement but not an IC intelligence requirement, FOD can write an FIR about the information but not an IIR.

threats identified on December 21 matched any IC requirements for issuing an IIR. However, the FOD member could not tell us what happened next, and we found no evidence that FOD drafted an IIR about this threat.[39]

On January 5, a FOD Mid-Atlantic Region member drafted an IIR about a different threat pertaining to January 6 and emailed it to another FOD member for review. The IIR stated that an individual posted online three times about how to avoid law enforcement detection and which equipment would be the most effective against the military and police. The IIR noted that the online posts received more than 1,800 views.

Yet, we found no evidence the FOD member who received the IIR via email reviewed the product at any point, and he informed us he did not remember what happened to the draft after he received it. Similarly, the IIR drafter did not remember what happened to the product. She initially told us that she might have shared the IIR with a senior FOD official to determine whether it matched IC requirements, but she could not locate any documentation confirming she shared it with this official or any additional individuals.

Even if FOD published IIRs on a classified system in the lead-up to January 6, those products may not have been as helpful as products posted on HSIN for state and local partners. These partners often have limited or no access to classified networks and might not have seen products on a classified system before violence on January 6 unfolded. In contrast, partners with access to HSIN can immediately obtain FIRs and IIRs posted there and share them with the appropriate officials responding to relevant threats and events.

I&A Shared Limited Threat Information about January 6 Events with State and Local Partners

One of I&A's primary responsibilities is to facilitate information sharing with its state and local partners. We determined that, on at least five occasions, I&A emailed threat information about January 6 events to state and local partners prior to the U.S. Capitol breach:

- On December 21, a FOD Mid-Atlantic Region member assigned to Washington D.C. emailed online forums with threat information related to January 6 to NTIC members. The FOD member informed NTIC that

[39] FOD also sent a tip with this information to OSCO. However, as previously discussed, an OSCO collector told FOD that she could not locate the threat online and that OSCO had to locate it before reporting on it. FOD never responded, and OSCO did not draft an OSIR based on this tip.

the online forums discussed bringing unpermitted weapons to Washington, D.C., evading law enforcement detection, and threatening Congress and politicians.[40] Later that day, an NTIC intelligence analyst sent a summary of threat information collected by FOD and the NTIC to the Metropolitan Police Department, including a map of the U.S. Capitol building's tunnel system that had been shared online.

- On January 5, the Federal Bureau of Investigation (FBI) published an intelligence product about individuals who established a "quick reaction force" in Northern Virginia. According to the FBI, these individuals planned to respond to violence during January 6 protests if they felt the "police were not doing their job." After learning about the FBI intelligence product, several I&A members shared the information with state and local partners:
  - A CETC analyst emailed the product to the U.S. Capitol Police and NTIC.
  - A FOD Mid-Atlantic Region member assigned to Washington, D.C. shared the product with the NTIC Executive Director.
  - A FOD Mid-Atlantic Region member assigned to Virginia shared the FBI intelligence product with two Virginia fusion centers.[41]

- On January 5, the FOD member in Washington D.C. also shared information with the NTIC Executive Director about armed individuals traveling to Washington, D.C. to incite violence. In response, the NTIC Executive Director said, "I got it from here." The FOD member told us he thinks NTIC shared this information with local law enforcement.

In all five of these instances, I&A personnel quickly informed state and local officials about threat information, which could have aided their operational response during the January 6 events. However, sharing information via email does not disseminate information as widely as publishing intelligence products, which are posted on HSIN and available to a broad range of state and local partners. Additionally, in three of these instances, I&A shared an intelligence product issued by another agency, rather than information it discovered during its own intelligence collection or analysis efforts. Despite the numerous threats I&A encountered in the weeks preceding January 6, I&A did not produce any intelligence products about the information before the U.S. Capitol breach.

[40] As previously discussed, the FOD member planned to draft an FIR about these threats, but we found no evidence it was drafted.
[41] This FOD member also asked an FBI contact for more information about the reporting. When we asked the FOD member if he received a response, he could not remember.

We did not identify any additional instances of I&A sharing threat information with state and local partners prior to the January 6 events. We issued a mandatory questionnaire to FOD field employees asking whether they shared related information with state and local partners prior to the January 6 events. No respondents indicated any additional instances of information sharing occurred. Further, we contacted certain individuals within the U.S. Capitol Police, Metropolitan Police Department, NTIC, FBI, and the Department of Interior to ask whether they received information from I&A prior to the January 6 events. NTIC did not respond to our request, and the other agencies said they did not receive any information from I&A. We also reviewed transcripts from secure chat rooms that I&A officials hosted or joined leading up to the U.S. Capitol breach. Although I&A personnel were present in the chat rooms, we did not note further sharing of threat information prior to the breach.

Conclusion

I&A is the only member of the IC statutorily tasked with delivering intelligence to state, local, and Federal partners, as well as developing intelligence from these partners for DHS and the IC. Despite these responsibilities, I&A was unable to provide its many state, local and Federal partners with timely, actionable, and predictive intelligence prior to the U.S. Capitol breach on January 6, 2021. I&A staff disagree about whether an intelligence product from I&A would have affected the outcome on January 6. Nonetheless, the issues we found during our review demonstrate the need for essential changes at I&A to ensure it is better equipped to respond to similar events in the future.

Recommendations

We recommend the Under Secretary for Intelligence and Analysis:

Recommendation 1: Provide enhanced annual training and guidance to OSCO staff reviewing the *Intelligence Oversight and Program Guidelines*, including all criteria for reporting open source intelligence information.

Recommendation 2: Develop and implement a process to provide new OSCO members with adequate training and guidance with input from experienced collectors or the Intelligence Training Academy.

Recommendation 3: Establish and implement a process to request and receive timely reviews for open source intelligence products when they relate to upcoming events or urgent threats.

Recommendation 4: Develop and implement policies, procedures, or guidance on the timely issuance of warning analysis, both strategic and tactical, about threats or upcoming events across I&A's mission areas.

Recommendation 5: Create and implement redundant capabilities for I&A to disseminate intelligence products addressing departmental threats, including FIRs and OSIRs.

Management Comments and OIG Analysis

I&A concurred with our recommendations and described corrective actions to address the issues identified in this report. Appendix B contains I&A's management comments in their entirety. We also received technical comments to the draft report and revised the report as appropriate. We consider these recommendations resolved and open. A summary of I&A's response to our recommendations and our analysis follows.

Recommendation 1: Provide enhanced annual training and guidance to OSCO staff reviewing the *Intelligence Oversight and Program Guidelines*, including all criteria for reporting open source intelligence information.

I&A's Comments to Recommendation 1: Concur. I&A's CETC OSCO employees performing open-source collections are required by the Under Secretary for I&A and CETC leadership to attend formal training at the DHS Intelligence Training Academy that includes (1) an introductory "Open-Source Intelligence (OSINT) Course" which addresses intelligence oversight, and (2) the "Open-Source Intelligence Report (OSIR) Workshop," which specifically addresses program guidelines as they relate to open-source intelligence reports and oversight. Additionally, in calendar year 2021, I&A increased its overall intelligence compliance program, which includes intelligence oversight training. Not only are all I&A staff required to take intelligence oversight training annually, in 2021, the Intelligence Training Academy also instituted a new approach to this annual requirement by emphasizing live, OSCO-specific, interactive training in online modules. In addition, I&A's Privacy and Intelligence Oversight Branch regularly trains I&A personnel on emerging compliance issues. I&A requests that OIG consider this recommendation resolved and closed.

OIG Analysis: We consider these actions responsive to the recommendation, which is resolved and open. We will close this recommendation when we receive evidence that I&A included all criteria for reporting open source intelligence in its enhanced training and guidance.

Recommendation 2: Develop and implement a process to provide new OSCO members with adequate training and guidance with input from experienced collectors or the Intelligence Training Academy.

I&A's Comments to Recommendation 2: Concur. Effective September 1, 2021, I&A employees assigned to open-source collection duties in OSCO are assigned a series of initial training courses that incorporate principles of intelligence oversight and legal guidance. This training was developed by the Intelligence Training Academy in consultation with IC partners, in order to better address the needs of OSCO members. It was initiated in collaboration with the IC Open Source Enterprise Program to address needs for DHS Open-Source Intelligence training and identify existing IC courses that could be used to support the I&A training development effort. I&A requests that OIG consider this recommendation resolved and closed.

OIG Analysis: We consider these actions responsive to the recommendation, which is resolved and open. We will close this recommendation when we receive evidence that I&A delivered training developed in consultation with experienced collectors or the Intelligence Training Academy to new OSCO members.

Recommendation 3: Establish and implement a process to request and receive timely reviews for open source intelligence products when they relate to upcoming events or urgent threats.

I&A's Comments to Recommendation 3: Concur. On August 31, 2021, I&A's Chief Information Officer in coordination with CETC (as memorialized in a memorandum provided under separate cover to the OIG on January 27, 2022), implemented a new OSIR processing system which reduces the time needed for reviewing and releasing OSIRs, while ensuring thorough review.

Currently, OSIRs do not need to be reviewed by personnel outside of OSCO prior to release, which increases the ability to disseminate products timely. The return to releasing OSIRs at the OSCO Branch level was documented in an I&A Deputy Under Secretary Intelligence Enterprise Operations memorandum to CETC on February 18, 2021. For content about which collectors seek additional oversight review, the on-site intelligence oversight officer engages in expedited review that can result in the collection, review, and dissemination of high profile threat reports within hours of discovery. Additionally, I&A anticipates that, by mid-February 2022, OSCO will have a fully staffed permanent leadership team in place, which will increase the number of highly-qualified personnel to review and release open source intelligence products.

I&A is also in the process of updating policies and standard operating procedures regarding the production of OSIRs, and anticipates formalizing the OSIR standard operating procedure in April 2022 and revising IA-900, "Official Usage of Publicly Available Information," dated January 13, 2015, which establishes the standards, guidelines, and processes for using publicly available information for research, collection, analysis, retention, citing, reporting, and dissemination. Estimated Completion Date: December 30, 2022.

OIG Analysis: We consider these actions responsive to the recommendation, which is resolved and open. We will close this recommendation when we receive evidence of I&A's updated standard operating procedures for production of OSIRs that include processes to request and receive timely reviews for upcoming events and urgent threats.

Recommendation 4: Develop and implement policies, procedures, or guidance on the timely issuance of warning analysis, both strategic and tactical, about threats or upcoming events across I&A's mission areas.

I&A's Comments to Recommendation 4: Concur. I&A's policy to produce finished intelligence, IA-901, "Production of Finished Intelligence," dated May 7, 2020, establishes the responsibilities and procedures within I&A for the production, review, approval, and dissemination of I&A finished intelligence products. This policy provides the parameters for an expedited process through which I&A is able to issue products related to an immediate threat to homeland security or other exigent crisis or situations. I&A's Intelligence Enterprise Operations and Intelligence Enterprise Readiness Offices are leading a review, which I&A intends to complete by April 2022, to determine whether any additional policy or procedural changes are required to modify intelligence production processes. I&A anticipates finalizing a correlating standard operating procedure that will implement at a more detailed level the updated IA-901 policy by the end of April 2022. I&A's Intelligence Enterprise Operations and Intelligence Enterprise Readiness Offices will also work with I&A's Strategy, Plans, and Policy Branch and OGC-ILD to provide clarifying guidance to ensure all staff are aware of these processes and parameters for developing and issuing products in such exigent circumstances. Estimated Completion Date: April 29, 2022.

OIG Analysis: We consider these actions responsive to the recommendation, which is resolved and open. We will close this recommendation when we receive evidence that I&A finalized new policy, procedures, or guidance on the timely issuance of warning analysis about threats or upcoming events.

Recommendation 5: Create and implement redundant capabilities for I&A to disseminate intelligence products addressing departmental threats, including FIRs and OSIRs.

I&A's Comments to Recommendation 5: Concur. To enhance I&A's capabilities to disseminate intelligence reports, I&A's Office of the Chief Information Officer, in coordination with FOD, is updating the tool used to issue FIRs to a web-based system, which is currently similar to I&A's tool used to produce OSIRs. Additionally, FIRs, OSIRs, and IIRs of value to state and local partners will also be disseminated via the HSIN - Intelligence platform. These enhancements will enable information sharing redundancies, and will make the dissemination of intelligence to key partners within and outside the Department more efficient and timelier. Estimated Completion Date: June 30, 2022.

OIG Analysis: We consider these actions responsive to the recommendation, which is resolved and open. We will close this recommendation when we receive evidence that I&A has finished implementing redundant capabilities, such as updating the tool used to issue FIRs to a web-based system and issuing certain products via HSIN.

Appendix A
Objective, Scope, and Methodology

The Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Public Law 107–296) by amendment to the *Inspector General Act of 1978*.

We initiated this review in response to questions about whether Federal intelligence and law enforcement organizations had, or should have developed and shared, information relating to the potential for violence during January 6, 2021 events. Our objective was to review I&A's responsibility for providing intelligence to law enforcement for the January 6, 2021 events at the U.S. Capitol, and whether and how I&A fulfilled its responsibility.

Throughout our fieldwork, we defined "January 6 events" as "any event, activity, or gathering, whether formal or informal, permitted or unpermitted, taking place in Washington, D.C., related to the January 6, 2021 counting of Electoral College votes by the U.S. Congress."

To identify intelligence that existed relating to January 6 events, we reviewed documents I&A produced in response to our formal request for:

- copies of any intelligence product, whether finished or unfinished, draft or final, relating to January 6 events that was received or collected by I&A in advance of the U.S. Capitol attack; and
- copies of any intelligence product, whether finished or unfinished, draft or final, relating to January 6 events that was generated or disseminated by I&A in advance of the U.S. Capitol attack.

We supplemented this effort by issuing a mandatory questionnaire to FOD field employees asking whether they created, accessed, disseminated, or were aware of intelligence relating to January 6 events; we then interviewed those who responded in the affirmative. We interviewed OSCO collectors and asked whether they created, accessed, disseminated, or were aware of intelligence relating to January 6 events. We also interviewed CTMC intelligence analysts and I&A leadership. We reviewed emails from relevant I&A officials and transcripts from secure chat rooms that I&A officials joined leading up to and during the January 6 event. We also contacted non-DHS officials in the U.S. Capitol Police, Metropolitan Police Department, NTIC, FBI, and the Department of Interior, to determine whether they received any threat information from I&A prior to the U.S. Capitol breach.

Additionally, we reviewed I&A policies to understand guidance and limitations that would have applied to intelligence relating to January 6 events.

We conducted this evaluation under the authority of the *Inspector General Act of 1978*, as amended, and according to the *Quality Standards for Inspection and Evaluation* issued by the Council of the Inspectors General on Integrity and Efficiency.

Appendix B
I&A Comments to the Draft Report

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

February 7, 2022

MEMORANDUM FOR: Joseph V. Cuffari, Ph.D.
Inspector General

FROM: John Cohen
Senior Official Performing the Duties of the Under Secretary
Office of Intelligence and Analysis

SUBJECT: Management Response to Draft Report: "I&A Identified Threats Prior to January 6, 2021, but Did Not Issue Any Intelligence Products before the U.S. Capitol Breach" (Project No. 21-023-SRE-I&A)

Thank you for the opportunity to comment on this draft report. The U.S. Department of Homeland Security (DHS or the Department) Office of Intelligence and Analysis (I&A) appreciates the work of the Office of Inspector General (OIG) in conducting its review and issuing this report.

I&A leadership agrees that the enhancement of the Organization's intelligence collection, production, and dissemination, especially related to its open source collection activities, is critical to improving I&A's ability to warn customers and partners of threats in the future. I&A appreciates the OIG's acknowledgement that I&A personnel identified, collected, and shared threat information associated with potential violence on January 6, 2021 with partners in the Washington, D.C. area on several occasions, and agrees that the recommendations in this report will help I&A strengthen its intelligence production and reporting processes. I&A remains committed to equipping the Homeland Security Enterprise with timely intelligence and information it needs to keep the homeland safe, secure and resilient.

Since the events of January 6, 2021, I&A has taken many actions to improve its ability to effectively identify, collect, and share threat information, including publicly-available information identified online. These actions have focused on (1) developing tools and procedures to enhance I&A's ability to identify and collect threat information and enhance intelligence, privacy, and civil rights and civil liberties oversight mechanisms, and (2) I&A's ability to ensure this information—whether in raw reports or via finished intelligence products—is efficiently shared.

During the last year, I&A convened more than 50 engagements to inform our partners about the threat environment, including biweekly calls with state and local law enforcement executives and national-level calls with a broad group of stakeholders on emerging threats. DHS also issued more than 80 intelligence products related to domestic violent extremism.

Additionally, I&A has taken actions to update and require specialized training for its personnel on technical tradecraft as well as legal, privacy, and civil liberties aspects of our intelligence work. I&A also issued comprehensive guidance and several training sessions to clarify for its officers I&A's authorities and responsibilities, and management oversight of collection and dissemination processes. Finally, I&A has improved the communication and collaboration between its Counterterrorism Mission Center and open-source collectors to help focus such efforts and leverage I&A's collective expertise.

The draft report contained five recommendations with which I&A concurs. Attached find our detailed response to each recommendation. We previously submitted technical comments addressing several accuracy, contextual, and other issues under a separate cover for OIG's consideration.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Attachment

Attachment: Management Response to Recommendations Contained in 21-023-SRE-I&A

The OIG recommended that the Under Secretary for I&A:

Recommendation 1: Provide enhanced annual training and guidance to OSCO [Open Source Collections Operations] staff reviewing the Intelligence Oversight and Program Guidelines, including all criteria for reporting open source intelligence information.

Response: Concur. I&A's Current and Emerging Threats Center (CETC)-OSCO employees performing open-source collections are required by the Under Secretary for I&A and CETC leadership to attend formal training at the DHS Intelligence Training Academy (ITA), that includes (1) an introductory "Open-Source Intelligence (OSINT) Course" which addresses intelligence oversight (IO), and (2) the "Open-Source Intelligence Report (OSIR) Workshop," which specifically addresses program guidelines as it relates to open-source intelligence reports and oversight. For example, following a fiscal year (FY) 2021 review of both the introductory OSINT course and the OSIR workshop for proper content, the OSIR Workshop was delivered to current OSCO employees on July 12-23, 2021. As of December 31, 2021, all OSCO employees have completed this two-course series of OSINT training. Further, to ensure that new and current I&A personnel complete training requirements promptly upon assignment to the CETC-OSCO Branch, ITA is prepared to provide additional OSINT training courses during FY 2022 to meet anticipated OSCO requirements. ITA, in coordination with CETC, plans to increase delivery of OSINT Courses to 20 and two iterations of the new OSIR Workshop in FY 2022.

Additionally, in calendar year (CY) 2021, I&A aggressively increased its overall intelligence compliance program, which includes IO training. Not only are all I&A staff required to take IO training annually, in 2021, ITA also instituted a new approach to this annual requirement by providing this training emphasizing live, OSCO-specific, interactive training over online modules. In addition, I&A's Privacy and Intelligence Oversight Branch (PIOB) regularly trains I&A personnel on emerging compliance issues. During CY 2021, I&A doubled its PIOB staff and modified its operational posture to an integrated preproduction model, which co-locates a dedicated Assistant Intelligence Oversight Officer with the OSCO collectors to provide readily accessible daily guidance and support throughout the process of accessing, collecting, and disseminating open-source intelligence. To supplement their training, PIOB also created for OSCO a wide array of practical products throughout CY 2021 designed to break down complex compliance guidelines into such as, easy-to-follow list of rules, fact sheets, checklists on lanyard cards, job aids, and multi-media training aides. Documentation corroborating the completion of these actions was provided under a separate cover to the OIG on January 27, 2022.

3

We request the OIG consider this recommendation resolved and closed, as implemented.

Recommendation 2: Develop and implement a process to provide new OSCO members with adequate training and guidance with input from experienced collectors or the Intelligence Training Academy.

Response: Concur. Effective September 1, 2021, I&A employees assigned to open-source collection duties within OSCO are assigned a series of initial training courses that incorporate principles of IO and legal guidance, as described above. This training was developed by the ITA in consultation with Intelligence Community (IC) partners, in order to better address the needs of OSCO members, and was initiated in collaboration with the IC Open Source Enterprise Program to address needs for DHS OSINT training and identify existing IC courses that could be used to support the I&A training development effort. This collaboration involved a curriculum review of a Defense Intelligence Agency open-source course that was similar to the needs of DHS. With a better understanding of current IC offerings, ITA, in coordination with CETC, built a release authority course in addition to the existing CETC courses that aligned to IC tradecraft using the I&A release processes. The ITA also confirmed the existing OSINT curriculum, revised the open-source intelligence report writing course and delivered the 'OSIR Workshop' described above.

The initial training plan includes a three-day "OSINT Course" featuring tradecraft, best practices, and tools, as well as the two-week "Open-Source Intelligence Report Workshop" that details the collection and exploitation of open-source information and development of Open Source Intelligence Reports and address IO. Following their completion of these courses, new OSCO personnel are also assigned under the direct supervision of OSINT Content Managers, which facilitates the practical application of learning objectives addressed in the training courses. This training was: (1) coordinated with I&A's Collection Management Division and PIOB; and (2) reviewed by the DHS Office of the General Counsel, the DHS Office for Civil Rights and Civil Liberties (CRCL), and the DHS Privacy Office (PRIV). Documentation corroborating the completion of these actions was provided under a separate cover to the OIG on January 27, 2022.

We request the OIG consider this recommendation resolved and closed, as implemented.

Recommendation 3: Establish and implement a process to request and receive timely reviews for open source intelligence products when they relate to upcoming events or urgent threats.

Response: Concur. On August 31, 2021, I&A's Chief Information Officer in coordination with CETC (as memorialized in CETC memorandum provided under separate cover to the OIG on January 27, 2022), implemented a new OSIR processing

system which reduced the time needed for reviewing and releasing OSIRs, albeit while ensuring thorough review.

Currently, OSIRs do not need to be reviewed by personnel outside of CETC OSCO prior to release, which increases the ability to disseminate products in a timely manner. The return to releasing OSIRs at the OSCO Branch level was documented in an I&A Deputy Under Secretary Intelligence Enterprise Operations memorandum to CETC on February 18, 2021 (provided under a separate cover to the OIG on February 1, 2022). For content that collectors wish to, or are required to, seek additional oversight review, the on-site IO officer, in close coordination with the DHS Office of the General Counsel-Intelligence Law Division (OGC-ILD), PIOB, CRCL and PRIV, engage in expedited review that can result in the collection, review, and dissemination of high profile threat reports within hours of discovery. Additionally, I&A anticipates that, by mid-February 2022, OSCO will have a fully staffed permanent leadership team in place, which will increase the number of highly-qualified personnel to review and release open source intelligence products. I&A is also in the process of updating policies and standard operating procedures (SOP) regarding the production of OSIRs, and anticipates formalizing the OSIR SOP in April 2022 and revising IA-900, "Official Usage of Publicly Available Information," dated January 13, 2015, which establishes the standards, guidelines, and processes for using Publicly Available Information, including publicly available social media platforms, for research, collection, analysis, retention, citing, reporting, and dissemination.

Estimated Completion Date (ECD): December 30, 2022.

Recommendation 4: Develop and implement policies, procedures, or guidance on the timely issuance of warning analysis, both strategic and tactical, about threats or upcoming events across I&A's mission areas.

Response: Concur. I&A's policy to produce finished intelligence, IA-901, "Production of Finished Intelligence," dated May 7, 2020, establishes the responsibilities and procedures within I&A for the production, review, approval, and dissemination of I&A finished intelligence products. This policy provides the parameters for an expedited process through which I&A is able to issue products related to an immediate threat to homeland security or other exigent crisis or situations. I&A's Intelligence Enterprise Operations (IEO) and Intelligence Enterprise Readiness (IER) Offices are leading a review, which I&A intents to complete by April 2022, to determine whether any additional policy or procedural changes are required to modify intelligence production processes and I&A anticipates finalizing a correlating SOP that will implement at a more detailed level the updated IA-901 policy by the end of April 2022. I&A's IEO and IER Offices, will also work with I&A's Strategy, Plans, and Policy Branch and OGC-ILD to provide clarifying guidance to ensure all staff are aware of these processes and parameters for developing and issuing products in such exigent circumstances.

5

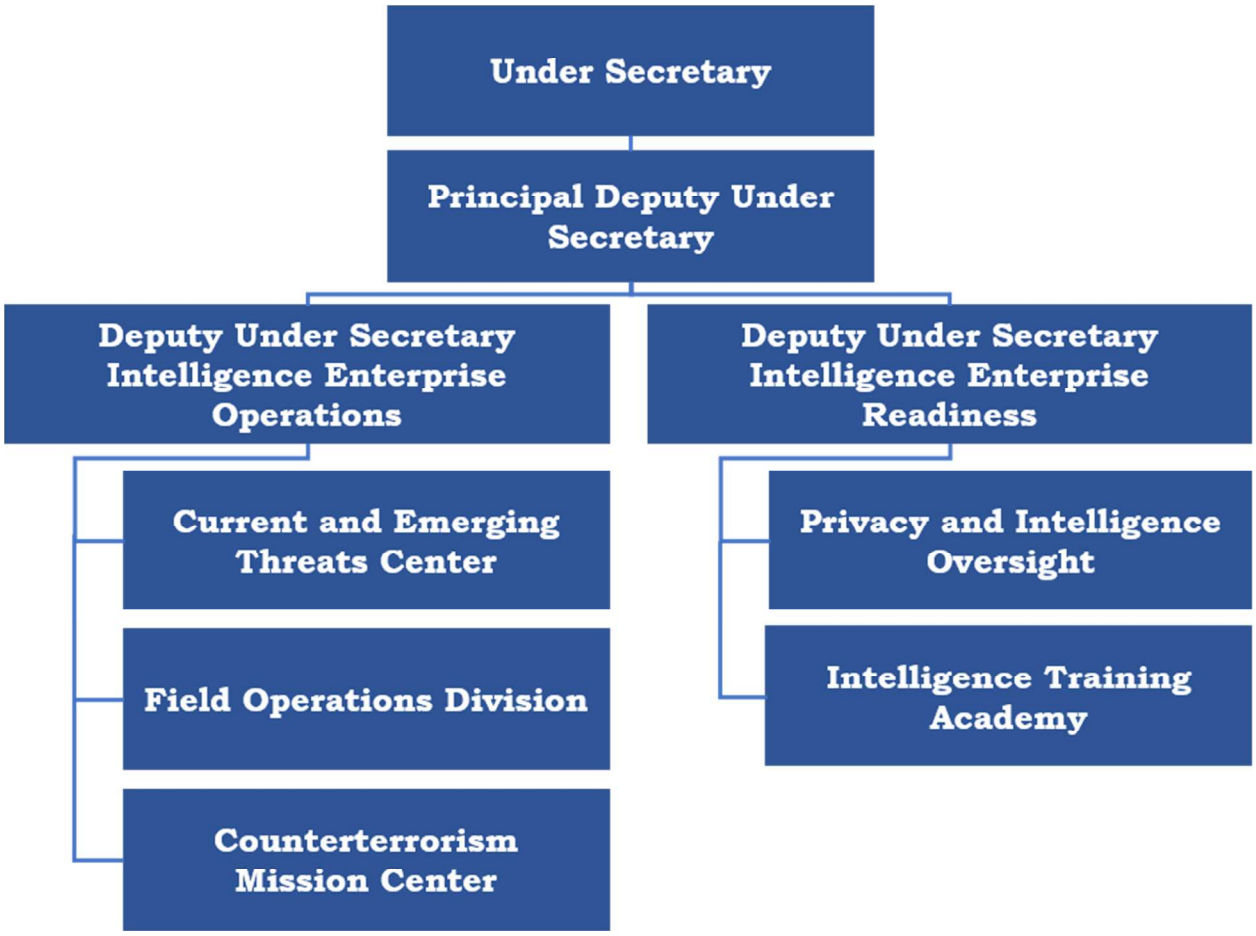
With respect to warning analysis, both strategic and tactical, I&A IEO and IER leadership will continue to work with our IC partners to ensure that I&A personnel have access to community expertise and training on conducting warning analysis, such as assessing indications, establishing warning problem sets, and conveying warning effectively.

ECD: April 29, 2022.

Recommendation 5: Create and implement redundant capabilities for I&A to disseminate intelligence products addressing departmental threats, including FIRs [field intelligence reports] and OSIRs.

Response: Concur. To enhance I&A's capabilities to disseminate intelligence reports, I&A OCIO, in coordination with the I&A's Field Operations Division, is updating the tool used to issue FIRs to a web-based system, which is currently similar to I&A's tool used to produce OSIRs. Additionally, FIRs, OSIRs, and Intelligence Information Reports of value to state and local partners will also be disseminated via the Department's secure, online Homeland Security Information Network – Intelligence platform. These enhancements will enable information sharing redundancies, and will make the dissemination of intelligence to key partners within and outside the Department more efficient and timelier. During CY 2021, CETC also doubled the number of Certified Release Authorities (CRA) in OSCO to build redundancy in that capability. CRAs are I&A personnel authorized by the Undersecretary of I&A to release I&A raw intelligence reports. ECD: June 30, 2022.

Appendix C
Organizational Chart of Relevant I&A Offices



Appendix D
January 6 Threats Identified by OSCO in Response to the RFI

Five OSCO collectors documented the following information in response to CTMC's RFI regarding the January 6 events.[42] This does not encompass all threat information identified by OSCO, FOD, and CTMC prior to the U.S. Capitol breach.

December 29, 2020

OSCO Collector 1

- On a forum thread with over 5,500 likes and over 250 comments, one user suggests [redacted] User also suggest [redacted] in D.C.

December 30, 2020

OSCO Collector 1

- Forum user post he intends to travel to D.C. with weapons; seeking others to join via "carpool".
- Forum user mentioned a group of women planning on bringing guns to D.C.

OSCO Collector 2

- Social media user advocates for marching on DC with guns if [POTUS] is not declared the winner on Jan 6th.
- Social media user claims to be bringing guns to protest, saying, [redacted]

OSCO Collector 3

- [redacted]

[42] The OIG did not edit the collectors' language when compiling information for this appendix.

- [redacted] Post has 73 upvotes.

[redacted]

OSCO Collector 4

- An individual discusses coming armed and meeting outside the city and then [redacted]
- Discussions of organizing in Virginia and then driving to DC armed together as the police/military won't be able to stop thousands of armed patriots
- Suggestions of using stun guns
- [redacted]

January 2

OSCO Collector 2

- Social media user advocating for protestors to [redacted]

OSCO Collector 3

- Forum user stated: [redacted]
- Forum user stated: [redacted]

- Several images are circulating depicting the Capitol Building and [redacted]

OSCO Collector 4

- [redacted] -Post received 257 comments, 907 likes, and 217 re-tweets
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- Lots of discussions of coming armed to DC as law enforcement [redacted], few anonymous posts mention of [redacted] Congress, several posts on 02 January 2021 from a dozen or so users [redacted]

January 3

OSCO Collector 1

- One forum user (OP[43]) post: [redacted]
  - Another user replied: [redacted]
  - A Second user replied to OP: [redacted]

OSCO Collector 5

- Users call (USPER[44]) 'Patriots' to congregate in DC on January 6th to retaliate against (USPER) BLM (USPER) ANTIFA . Advocate violence and raping children.

[43] OP refers to the original poster.
[44] USPER refers to a U.S. person.

Appendix E
I&A Timeline Related to the January 6 Events

LEGEND

- Field Operations Division
- Counterterrorism Mission Center
- Current and Emerging Threats Center (including the Open Source Collection Operations branch)
- Intelligence Law Division
- U.S. Capitol Breach

Dec 21 2020 12:26 PM
A Field Operations Division (FOD) member shared with other FOD staff an online threat about an individual threatening to shoot and kill protesters at upcoming rallies related to the presidential election. A supervisor recommended issuing a Field Intelligence Report (FIR) about the threat, but FOD never drafted the product. The supervisor also recommended sending a tip to the Current and Emerging Threats Center's (CETC) Open Source Collection Operations branch (OSCO) about the threat.

Dec 21 2020 2:39 PM
A FOD member emailed online forums with threat information related to January 6 to the National Capital Region Threat Intelligence Consortium (NTIC). The FOD member informed NTIC that the online forums discussed bringing unpermitted weapons to Washington, D.C., evading law enforcement detection, and threatening Congress and politicians.

Dec 21 2020 3:15 PM
FOD shared a tip with OSCO about the online threat to shoot and kill protesters at the upcoming rallies. According to the tip, the individual informed members of an online discussion group that he planned to kill at least 50 individuals.

Dec 21 2020 3:10 PM
The FOD member informed his supervisor that he and a colleague would write an FIR about the threats posted in the online forums, but never drafted the product.

Dec 21 2020 3:47 PM
An OSCO collector told FOD that she could not locate the [redacted] and that OSCO had to [redacted] However, FOD never responded and OSCO did not draft an Open Source Intelligence Report (OSIR) based on this tip.

Dec 29 2020 9:52 AM
CTMC sent a request to OSCO to research threat information regarding January 6 events.

Dec 30 2020
An OSCO collector identified an individual online who stated [redacted]

Dec 30 2020
An OSCO collector noted that an individual online claimed that there would not be enough law enforcement officers to stop the number of armed people arriving in the area.

Jan 02 2021
An OSCO collector discovered that several images of the U.S. Capitol building and its [redacted] were circulating online.

Jan 02 2021
An OSCO collector documented that there were posts by individuals online calling for the [redacted] of the U.S. Congress and saying they [redacted]

Jan 02 2021 8:21 PM
In a Microsoft Teams Chat discussion, an OSCO collector said, "Also I found a map of all the exits and entrances to the capitol building. I feel like people are actually going to try and hurt politicians. Jan 6th is gonna be crazy, not to mention the inauguration. Watch us get surged for that lol."

Jan 02 2021 11:17 PM
In a Microsoft Teams Chat discussion, an OSCO collector said, "Like there's these people talking about hanging Democrats from ropes like wtf."

Jan 03 2021 2:53 AM
In a Microsoft Teams Chat discussion, an OSCO collector said, [redacted]

Jan 04 2021 1:38 PM
A CTMC intelligence analyst informed other CTMC employees that they were tasked with analyzing indicators of potential protest-related violence in Washington, D.C. The CTMC intelligence analyst said this analysis "is not intended to be published as a formal product at this time," and it will instead be used for an internal briefing.

Jan 04 2021 2:24 PM
An OSCO collector completed a draft OSIR about individuals planning to sacrifice their lives during violence on January 6. The collector noted that an individual suggested storming the U.S. House of Representatives chamber in the U.S. Capitol and mentioned grievances about police in Washington, D.C.

Jan 04 2021 3:02 PM
The OSCO member sent a message to other OSCO employees explaining that he reevaluted the information in the draft OSIR and decided the threats were hyperbole and should not be reported.

Jan 05 2021 8:59 AM
An OSCO collector completed a draft OSIR about an individual posting online about traveling to Washington, D.C. for January 6 events [redacted] and searching for parking locations for other armed individuals.

Jan 05 2021 10:02 AM
FOD completed a draft Intelligence Information Report about January 6 that stated an individual posted online three times about how to avoid law enforcement detection and which equipment would be the most effective against the military and police. FOD does not recall what happened to the draft product.

Jan 05 2021 10:54 AM
The OSCO collector who drafted the OSIR earlier in the morning informed a colleague that he spoke with the Intelligence Law Division (ILD) and received clearance to disseminate the OSIR.

Jan 05 2021 2:38 PM
A FOD member shared information about armed individuals traveling to Washington, D.C. to incite violence with the NTIC Executive Director.

Jan 05 2021 4:02 PM
A CETC analyst emailed an FBI intelligence product about January 6 events to the U.S. Capitol Police and NTIC.

Jan 05 2021 4:37 PM
Another FOD member emailed the FBI intelligence product to two Virginia fusion centers.

Jan 06 2021 8:15 AM
CTMC briefed I&A leadership on indicators of potential violence in Washington, D.C. during the January 6 events.

Jan 06 2021 11:32 AM
FOD provided two additional tips about threats to Washington, D.C. Both tips referenced social media content instructing individuals to [redacted] One of the tips suggested individuals [redacted] OSCO did not draft an OSIR based on these tips.

Jan 08 2021
OSCO published the OSIR drafted on January 5.

Jan 04 2021 10:16 PM
In a Microsoft Teams Chat discussion, an OSCO collector said, "I found a group of dudes who arrived in DC for the 6 JAN event and [redacted] are like they are going to battle..."

Jan 05 2021 9:57 AM
CTMC identified seven out of eight indicators of potential violence associated with the protests planned for January 6, but did not draft an intelligence product about the potential violence.

Jan 05 2021 2:03 PM
FOD provided a tip to OSCO about a social media user calling for people to come to Washington, D.C. to counter the protests and stated, [redacted]

Jan 05 2021 3:18 PM
Following the tip, OSCO researched the social media account and informed FOD it was "unable to find any derogatory information."

Jan 05 2021 4:07 PM
A FOD member emailed the FBI intelligence product to the NTIC Executive Director.

Jan 06 2021 12:16 AM
ILD emailed OSCO collectors and supervisors summarizing why the OSIR drafted on January 5 met I&A's reporting guidelines.

Jan 06 2021 11:29 AM
FOD provided a tip about a social media user claiming the Proud Boys planned to shut down the Washington, D.C. water system.

Jan 06 2021 2:15 PM
Rioters breached the U.S. Capitol building.

Jan 06 2021 2:53 PM
OSCO notified FOD that the tip about shutting down the Washington, D.C. water system did not meet its reporting threshold.

Appendix F
Office of Inspector General Major Contributors to This Report

Erika Lang, Assistant Inspector General for Inspections and Evaluations
Brendan Bacon, Lead Inspector
Gregory Flatow, Lead Inspector
Adam Brown, Senior Inspector
Anthony Crawford, Intelligence Officer
Margaret Gersh, Senior Intelligence Analyst
Rebecca Blaskey, Attorney Advisor to the Inspector General
James Lazarus, Attorney Advisor to the Inspector General
Jennifer Berry, Independent Referencer

Appendix G
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chiefs of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Under Secretary for Office of Strategy, Policy and Plans
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
I&A Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

ADDITIONAL INFORMATION AND COPIES

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.
Follow us on Twitter at: @dhsoig.

OIG HOTLINE

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive, SW
Washington, DC 20528-0305