

**The Office for Bombing
Prevention Needs to
Improve Its Management and
Assessment of Capabilities to
Counter Improvised Explosive
Devices**





OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

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

March 29, 2022

MEMORANDUM FOR: Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency

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

JOSEPH V
CUFFARI

Digitally signed by JOSEPH V CUFFARI
Date: 2022.03.28 17:48:09 -04'00'

SUBJECT: *The Office for Bombing Prevention Needs to Improve Its Management and Assessment of Capabilities to Counter Improvised Explosive Devices*

For your action is our final report, *The Office for Bombing Prevention Needs to Improve Its Management and Assessment of Capabilities to Counter Improvised Explosive Devices*. We incorporated the formal comments provided by your office.

The report contains three recommendations aimed at improving the Cybersecurity and Infrastructure Security Agency's Office for Bombing Prevention's management and assessment of countering improvised explosive devices. Your office concurred with all three recommendations. Based on information provided in your response to the draft report, we consider recommendations 1 through 3 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 and of the disposition of any monetary amounts. Please send your closure request to OIGAuditsFollowup@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 the report on our website for public dissemination.

Please call me with any questions, or your staff may contact Bruce Miller, Deputy Inspector General for Audits, at (202) 981-6000.

Attachment



DHS OIG HIGHLIGHTS

The Office for Bombing Prevention Needs to Improve Its Management and Assessment of Capabilities to Counter Improvised Explosive Devices

March 29, 2022

Why We Did This Audit

OBP's primary mission is to protect life and critical infrastructure by building capabilities in the public and private sectors to prevent, protect against, respond to, and mitigate bombing incidents. We conducted this audit to determine to what extent OBP manages and assesses national capabilities to counter IEDs.

What We Recommend

We made three recommendations to improve OBP's management and assessment of C-IED capabilities.

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

The Cybersecurity and Infrastructure Security Agency's (CISA) Office for Bombing Prevention (OBP) needs to improve its management of the Department of Homeland Security's counter-improvised explosive devices (C-IED) efforts, as well as its assessment of national, regional, and state C-IED capabilities.

Although designated to lead day-to-day implementation of *Presidential Policy Directive 17: Countering Improvised Explosive Devices* within DHS, OBP is not managing component participation or tracking milestone completion dates as required. This occurred because it does not have a policy delineating its roles and responsibilities in leading C-IED efforts across the Department. In addition, although required by its *Counter-IED Resource Guide*, OBP does not have the necessary data to assess and report on national, regional, and state C-IED capabilities. Specifically, OBP's C-IED capability data is outdated because it does not have a policy requiring outreach to first responder special units to update this data. OBP also does not incorporate vital data from its programs and training into its capability assessments. Finally, OBP cannot generate automated C-IED capability reports to identify national, regional, and state C-IED gaps because its systems are not integrated and do not have the functionality to generate comprehensive reports at all levels.

Until OBP improves its management of DHS' C-IED efforts and its assessment of C-IED capabilities, it cannot effectively build awareness and help protect the Nation against the threat posed by IED attacks.

CISA Response

CISA concurred with all three recommendations.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Background

During the past few decades, improvised explosive devices (IED) have become a priority threat to national security — growing in frequency, magnitude, and complexity since the 9/11 attacks.¹ Within the Department of Homeland Security, the Cybersecurity and Infrastructure Security Agency's (CISA) Office for Bombing Prevention (OBP) is responsible for leading the Department's efforts to protect against IED attacks in the United States, and to build national, regional, and state awareness of threats posed by IEDs.

In February 2013, President Obama issued *Presidential Policy Directive 17: Countering Improvised Explosive Devices* (PPD-17), setting the national policy for counter-IED (C-IED) efforts. To address PPD-17 C-IED efforts, a Federal Interagency Joint Program Office was established. In March 2013, the Joint Program Office — administered by the Attorney General through the Federal Bureau of Investigation and comprising senior executives from the Department of Defense, Department of State, Department of Justice, Office of the Director of National Intelligence, and DHS — issued the *PPD-17 Implementation Plan*. This plan was updated in May 2019 to coordinate and track assigned tasks among its Federal partners that include the Department of Defense, Department of State, Department of Justice, Office of the Director of National Intelligence, DHS, and others to mitigate IED attacks. Within DHS, CISA charged OBP with overseeing the day-to-day implementation of PPD-17 and helping accomplish the following four strategic goals from PPD-17:

- 1) Reduce adversaries' access to IED materials.
- 2) Disrupt IED facilitation networks and interdict plots before threats become imminent.
- 3) Safeguard people, protect critical infrastructure and soft targets, and minimize consequences of IED incidents.
- 4) Enhance coordination and capacity-building to increase the impact and sustainment of the C-IED mission.

In 2020, the Joint Program Office issued *PPD-17 Implementation Plan Appendix B: Plans of Action for Objectives and Key Tasks* to help achieve the PPD-17 strategic goals. In particular, the plan assigned Federal agencies key tasks and individual milestones to complete the goals. As of September 2021, 10 DHS components: Countering Weapons of Mass Destruction; U.S. Customs and Border Protection; Cybersecurity and Infrastructure Security Agency; Federal Emergency Management Agency; U.S. Immigration and Customs Enforcement; Management Directorate; Science and Technology Directorate; Transportation

¹ *Countering Improvised Explosive Devices Implementation Plan*, Joint Program Office, May 10, 2019.



OFFICE OF INSPECTOR GENERAL Department of Homeland Security

Security Administration; United States Coast Guard; and United States Secret Service were assigned objectives and key tasks.

As part of its mission, OBP is also responsible for assessing the C-IED capabilities at the national level for first responder special units, such as bomb squads, explosives detection canine teams, dive teams, and special weapons and tactics (SWAT) teams throughout the United States (see Figure 1). OBP is responsible for systematically identifying and assessing capabilities through its National C-IED Capabilities Analysis Database (NCCAD). The database is designed to provide a snapshot of the Nation's C-IED preparedness by collecting information about personnel, equipment, and training required to better understand C-IED capabilities. NCCAD is also intended to provide decision makers with a comprehensive overview of C-IED capabilities that can be used to influence policy, assign resources, and respond to emerging IED threats.



Figure 1. First Responder Special Units
Source: DHS OIG obtained from internet

We conducted this audit to determine to what extent OBP manages and assesses national capabilities to counter IEDs.

Results of Audit

OBP Needs to Improve Its Management of DHS' C-IED Efforts

OBP is responsible for leading the day-to-day implementation of PPD-17 and coordinating the Department's C-IED efforts. This includes confirming participation and ensuring the DHS components assigned key objectives and tasks provide timely updates on their progress.

OBP needs to improve how it manages component participation. Specifically, although required, OBP has not identified the necessary DHS component representatives for their assigned PPD-17 key tasks or ensured that all representatives who have been identified are regularly participating in PPD-17 activities. As of September 2021, just 5 of the 10 DHS components were fully participating in efforts to achieve PPD-17's strategic goals, as shown in

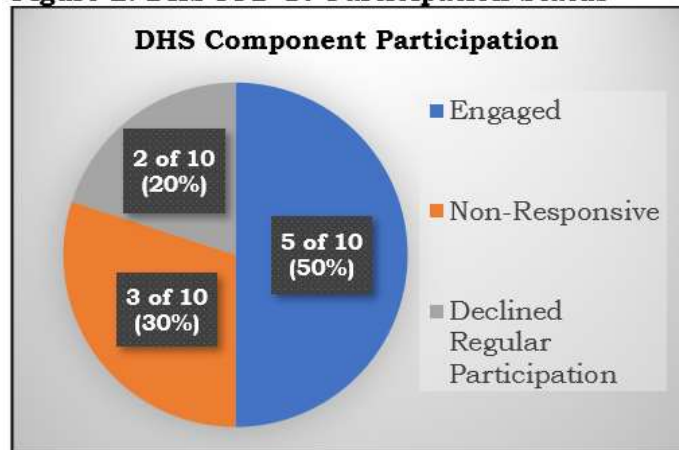


OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Figure 2. Of the remaining components, three did not respond to OBP's requests to participate and two declined to regularly participate, citing competing priorities for resources and a lack of C-IED applicability to their component's mission and operations. OBP made attempts to contact the three non-responsive components without requesting support from CISA, but OBP was not successful.

Figure 2. DHS PPD-17 Participation Status



Source: DHS OIG analysis of OBP data

Additionally, OBP does not always track DHS component progress, as required. As of May 2021, OBP was not tracking DHS components' progress in completing their assigned PPD-17 objectives and key task milestones. After the audit team brought the issue to OBP's attention, OBP began using its Plan of Action Milestone Tracker in June 2021 to track component progress. However, as of September 2021, OBP still had not collected updates for 19 of 112 key task milestones with planned completion dates on or prior to June 30, 2021. In fact, 2 of 19 key task milestones are classified as "critical — must do and time sensitive" requirements and must be completed in 1 to 3 years to secure the United States from IED incidents and their consequences. These critical tasks were determined to be significant towards advancing U.S. C-IED policy as established by the Joint Program Office and include items such as evaluating IED protective measures and identifying gaps related to the implementation of PPD-17.

OBP has not successfully managed component participation or tracked component progress because it does not have a policy that clearly delineates its roles and responsibilities for leading the day-to-day coordination and implementation efforts across DHS for PPD-17. Specifically, OBP does not have a formalized process for resolving problems with DHS components not being responsive to requests for participation to ensure representatives are assigned to key tasks and their associated milestones. Additionally, there is no formal policy specifying how often OBP must track and update its internal records on the status of all PPD-17 milestones assigned to DHS components. As a result, DHS' ability to identify and counter critical IED threats is diminished.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

OBP Cannot Assess and Report on National, Regional, or State C-IED Capabilities

According to *OBP’s Counter-IED Resource Guide*, OBP systematically identifies and assesses the Nation’s capabilities to counter IED threats. OBP uses its NCCAD to collect information about personnel, equipment, and training required to better understand C-IED capabilities. First responder special units throughout the United States can access the NCCAD to update their C-IED capability data on personnel, equipment, and training.

However, OBP does not have the necessary data or analytical information technology (IT) systems to assess and report C-IED capabilities at the national, regional, or state level. Specifically, 2,632 of 2,878 (91 percent) of first responder special units included in NCCAD have not made the updates used to generate C-IED capability reports since December 31, 2019, as shown in Table 1.

Table 1. First Responder Special Unit Updates since December 31, 2019

First Responder Special Units	First Responder Special Units in NCCAD	C-IED Assessments Not Updated	Percent Not Updated
Dive Team	417	375	90%
SWAT	1,431	1,352	94%
Canine	549	473	86%
Bomb Squad	481	432	90%
TOTAL	2,878	2,632	91%

Source: DHS OIG analysis of OBP’s NCCAD data as of March 3, 2022

Additionally, OBP’s C-IED capability assessments do not incorporate vital data from its other programs and training activities, such as:

- Multi-Jurisdiction Improvised Explosive Device Security Planning Program, which identifies C-IED roles, responsibilities, and capability gaps within individual first responder special units in multi-jurisdictional planning areas.
- Technical Resource for Incident Prevention (*TRIPwire*), which provides information about evolving IED tactics, techniques, procedures, incident lessons learned, and counter-IED preparedness for first responders, the private sector, and others.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

- Training that identifies needs for individual first responder special units highlighting strengths and weaknesses in abilities to counter IED threats.

Lastly, OBP's NCCAD system can only generate automated C-IED reports identifying gaps in personnel, organization, equipment, training, and exercises at the first responder special unit level and not at the national, regional, or state level. For example, after requesting national, regional, and state level C-IED capability reports, OBP was only able to provide us with a single state-level report. Moreover, according to OBP officials, the state-level report was developed manually and took more than 6 hours to produce. When we requested additional national, regional, or state C-IED capability reports, OBP officials stated they were not able to provide them due to lack of automated reporting and the time-consuming manual process involved in developing such reports.

These capability assessment challenges occurred because OBP does not have a policy requiring outreach to first responder special units in NCCAD to update their C-IED capability data. Furthermore, OBP's data is not integrated and NCCAD does not have the functionality to generate a complete picture of C-IED readiness at all levels.

To correct the deficiencies noted, OBP needs to improve its management of C-IED activities within the Department and its assessment of C-IED capabilities. OBP's management challenges diminish DHS' ability to identify and counter critical IED threats, as well as its ability to achieve its mission and establish a national C-IED policy. Additionally, capability assessment weaknesses prevent OBP from having a complete, accurate, and comprehensive picture of the Nation's C-IED capabilities and preparedness efforts. Without improvements, OBP cannot effectively build awareness and help protect the Nation against the threat posed by IED attacks.

Recommendations

We recommend the Cybersecurity and Infrastructure Security Agency Director:

Recommendation 1: Issue policy that clearly delineates the Office for Bombing Prevention's day-to-day responsibilities in leading Presidential Policy Directive 17 coordination and implementation efforts across DHS, including a process for identifying, tracking, and elevating participation issues, as well as tracking milestones quarterly.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Recommendation 2: Issue policy requiring the Office for Bombing Prevention to contact its first responder special units on an annual basis and retain records for these efforts.

Recommendation 3: Integrate its C-IED data sources and modernize its NCCAD reporting system to generate automated reports at the national, regional, and state level.

Management Comments and OIG Analysis

CISA concurred with all three recommendations and provided comments to the draft report. We included a copy of CISA's management comments in its entirety in Appendix A. CISA also provided technical comments to our draft report and we incorporated these comments, as appropriate.

CISA Response to Recommendation 1: Concur. The CISA Office of Strategy, Policy, and Plans (OSPP) will issue an internal policy that delineates OBP's day-to-day responsibilities. OBP will also continue to convene quarterly DHS IED Working Group meetings to solicit and record input from components on the status of milestones. Estimated Completion Date (ECD): August 31, 2022.

OIG Analysis: We consider these actions responsive to the recommendation, which is resolved and open. This recommendation will remain open until CISA issues an internal policy that delineates OBP's day-to-day responsibilities.

CISA Response to Recommendation 2: Concur. CISA OSPP will draft policy requiring contact with all first responder special units on an annual basis and establish guidelines for the documentation and retention of these engagements. ECD: August 31, 2022.

OIG Analysis: We consider these actions responsive to the recommendation, which is resolved and open. This recommendation will remain open until we receive the CISA OSPP policy requiring contact with all first responder special units on an annual basis and retention of records.

CISA Response to Recommendation 3: Concur. CISA took NCCAD offline and began migrating it to a new Amazon Web Services (AWS) Cloud-based operating environment. OBP is also working with CISA procurement to prepare a contract to finalize development, implementation, and program sustainment of the AWS Cloud-based operating environment. CISA plans to initiate technical deployments to include data visualization capabilities, the data warehouse, NCCAD data feed, incident data feed, and the uploading of



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

spreadsheets that contain a wide range of C-IED programmatic data. These actions are scheduled to be completed and reach Initial Operational Capability by March 2023. ECD: March 31, 2023.

OIG Analysis: We consider these actions responsive to the recommendation, which is resolved and open. This recommendation will remain open until CISA demonstrates the capability to generate automated reports at the national, regional, and state level.

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*.

Our audit objective was to determine to what extent OBP manages and assesses national capabilities to counter IEDs. To achieve our objective, we reviewed Federal laws, regulations, requirements, and program guidance associated with OBP's C-IED efforts. We also reviewed and analyzed prior audits and reports, testimonies, and hearings related to the audit objective.

We conducted interviews with key officials from OBP's executive leadership and its branches: Counter-IED Strategy, Integration, and Communications, Counter-IED Analysis and Planning, Counter-IED Information Sharing, and Counter-IED Training and Awareness. Additionally, we conducted interviews with officials in the following DHS components with assigned responsibilities in implementing PPD-17: Countering Weapons of Mass Destruction, U.S. Customs and Border Protection, CISA, Federal Emergency Management Agency, U.S. Immigration and Customs Enforcement, Science and Technology Directorate, Transportation Security Administration, U.S. Coast Guard, and U.S. Secret Service. We did not meet with the Management Directorate, Office of Biometric Identity Management, because it was incorporated as a PPD-17 stakeholder after our May 2021 evaluation of participation data, but we did include the component's data in our analysis as of September 2021.

In performing our audit, we identified Federal requirements regarding management's responsibility for internal control and managing the risks for fraud. We further analyzed the design of controls and operations related to OBP's C-IED activities from 2018 through 2021. We identified deficiencies affecting OBP's management of national C-IED policy implementation and reporting of C-IED national, regional, and state capabilities, as discussed in the body of this report.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

We evaluated OBP's management of C-IED participation within the Department through analyses of OBP's data about DHS component participation for PPD-17 implementation activities. We analyzed OBP's participation data as of September 2021 to identify the number of DHS components for which OBP had not yet identified a representative for PPD-17 key tasks or for which a representative was identified but declined to regularly participate in PPD-17 activities.

We assessed the reliability of OBP's participation data through interviews with representatives from six DHS components identified in the *PPD-17 Plans of Action for Objectives and Key Tasks*, issued September 2020. These interviews validated the accuracy of OBP's PPD-17 participation data. We determined the data was complete and accurate for assessing OBP's management of DHS component participation within PPD-17.

We assessed OBP's management of DHS component milestones through analyses of the PPD-17 key task milestone assignments made to components as of May 2021 and September 2021. We reviewed and assessed the planned completion dates for each of the milestones on both dates. We identified the number of milestones that exceeded the planned completion dates and were missing a status update. We further categorized milestones based on their timeframe for completion as either *Category A: Critical – Must Do and Time Sensitive, 1-3 Years* or *Category B: Necessary – Needed but Not Time Critical, 1-3 Years and 3-5 Years*.

We assessed the reliability of OBP's PPD-17 Plan of Action Milestone Tracker data through comparison of milestones to C-IED working group meeting records. We judgmentally selected 12 key task milestones and validated that the status of those milestones matched with the status description provided in the applicable C-IED working group meeting summaries. We determined the data to be complete and accurate as of September 2021 for assessing OBP's tracking of DHS PPD-17 milestones.

We evaluated OBP's ability to assess first responder special C-IED capabilities at the national, regional, and state levels through analyses of OBP's NCCAD user database to determine the frequency with which first responder special units update their capabilities information. We relied on OBP's NCCAD database for data about first responder special unit capability reporting. Additionally, due to the absence of national and regional C-IED capability reports, we only reviewed and analyzed OBP's available first responder special units and state reports to determine its reporting functionality. Given that bomb squads are the only first responder special units required to be accredited by the Federal Bureau of Investigation (FBI), we compared the FBI's accredited Bomb Squad List to OBP's NCCAD data to determine its reliability.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

We determined that the Bomb Squad data universe was complete and accurate.

Following our data reliability assessment of OBP's participation, milestone tracking, and capability assessment reporting, we determined the data applicable to our audit objective was sufficiently reliable to support the findings, recommendations, and conclusions in the report.

We conducted this performance audit between January 2021 and March 2022 pursuant to the *Inspector General Act of 1978, as amended*, and according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security


Appendix A
CISA Comments to the Draft Report



U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Office of the Director
Washington, DC 20528

March 15, 2022

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

FROM: Jen Easterly 
Director
Cybersecurity and Infrastructure Security Agency

SUBJECT: Management Response to Draft Report: “The Office for Bombing Prevention Needs to Improve Its Management and Assessment of Capabilities to Counter Improvised Explosive Devices” (Project No. 21-009-AUD-CISA)

Thank you for the opportunity to comment on this draft report. The Cybersecurity and Infrastructure Security Agency (CISA) appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing this report.

CISA is pleased to note OIG’s positive recognition of the Office for Bombing Prevention’s (OBP) important role to protect life and critical infrastructure by building capabilities in the public and private sectors to prevent, protect against, respond to, and mitigate bombing incidents and countering improvised explosive devices (C-IED). Bombings are an enduring tactic used in terrorism and targeted violence that pose a threat to our nation and the American public, including critical infrastructure, mass gatherings, and crowded spaces. For more than 15 years, OBP has played a role to build capacity and coordinate C-IED in the U.S. Department of Homeland Security (DHS) and across the United States.

OBP’s mission remains critical in light of the enduring risk posed by bombings and recent increase in domestic incidents, including bombings and bomb threats. For example, the U.S. saw a 71 percent increase in domestic bombings in 2020 and a nearly 56 percent increase in overall explosion incidents since 2015, with over 15,000 total explosives-related incidents per year. Additionally, Historically Black Colleges and Universities were targeted with over 60 bomb threats from January to February 2022. In 2021, OBP was elevated from a Branch-level program to a Sub-Division, as CISA took action to enhance its organizational and operation model following passage of the Cybersecurity and Infrastructure Security Agency Act of 2018 (Pub Law No. 115-278). OBP is working diligently to fulfill its more prominent role and responsibilities in that context.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

C-IED is a challenging mission with many stakeholders that requires effective planning, coordination, and prioritization. Coordination between CISA, DHS Components and Lines of Business, and other federal Departments and Agencies, including Sector Risk Management Agencies, remains a top priority for CISA. CISA's role as lead DHS Component for the implementation of Presidential Policy Directive 17, "Countering IEDs" (PPD-17) along with OBP's role as: (1) Chair of the DHS Improvised Explosive Devices (IED) Working Group; and (2) Deputy Administrator of the interagency Joint Program Office for C-IED, uniquely position OBP to enhance security and resilience capacity for C-IED and to coordinate efforts for maximum impact. CISA remains committed to enhancing the nation's ability to prevent, protect against, respond to, and mitigate bombing incidents that target critical infrastructure; the private sector; and federal, state, local, tribal, and territorial entities.

The draft report contained three recommendations with which CISA concurs. Attached find our detailed response to each recommendation. CISA 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



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

**Attachment: Management Response to Recommendations
Contained in 21-009-AUD-CISA**

OIG recommended that the CISA Director:

Recommendation 1: Issue policy that clearly delineates the Office for Bombing Prevention's day-to-day responsibilities in leading Presidential Policy Directive 17 coordination and implementation efforts across DHS, including a process for identifying, tracking and elevating participation issues, as well as tracking milestones quarterly.

Response: Concur. The CISA Office of Strategy, Policy, and Plans (OSPP) will issue an internal policy that delineates OBP's day-to-day responsibilities. In the interim, CISA has taken steps to internally codify consistent tracking and reporting of deficiencies for remediation. In October 2020, for example, CISA OBP developed a tracking mechanism for milestone progress based on input from U.S. Customs and Border Protection, Countering Weapons of Mass Destruction Office, Federal Emergency Management Agency, Office of Intelligence and Analysis, U.S. Immigration and Customs Enforcement, Science and Technology Directorate, Transportation Security Administration, U.S. Coast Guard, U.S. Secret Service, Office of Operations Coordination, and Office of Strategy, Policy, and Plans. CISA OBP will also continue to convene quarterly DHS IED Working Group meetings to solicit and record input from Components on the status of milestones. Estimated Completion Date (ECD): August 31, 2022.

Recommendation 2: Issue policy requiring the Office for Bombing Prevention to contact its first responder special units on an annual basis and retain records for these efforts.

Response: Concur. From June 2021 to January 2022, CISA OBP met with the National Bomb Squad Commander's Advisory Board and the Federal Bureau of Investigation's (FBI) Hazardous Devices School (HDS) to agree upon a mechanism that will ensure current and complete data population from all HDS-accredited Public Safety Bomb Squads. Accordingly, during the May 2022 Bomb Squad Commander's Conference, bomb squads will be informed that as a prerequisite to attend training at FBI's HDS, units will have to present a certificate demonstrating they have updated the National Counter Improvised Explosive Device Capabilities Analysis Database (NCCAD) within the previous 12 months. This agreement will be codified by a CISA/FBI Memorandum of Understanding. In addition, CISA OSPP will draft policy requiring contact with all first responder special units on an annual basis and establishing guidelines for the documentation and retention of these engagements. ECD: August 31, 2022.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Recommendation 3: Integrate its C-IED data sources and modernize its NCCAD reporting system to generate automated reports at the national, regional, or state level.

Response: Concur. In the Fall of 2019, CISA determined that the NCCAD operating system was outdated, vulnerable to cyber security threats, and unsustainable, and subsequently took the system offline and began migrating the NCCAD database to a new Amazon Web Services (AWS) Cloud-based operating environment. CISA then began collaborating with United States Digital Service to identify a “minimum viable product” solution to OBP’s data reporting and management requirements, and awarded a contract on September 21, 2020, to begin development and implementation of that product. This contract will conclude in June 2022, and CISA OBP is working with CISA procurement to prepare a follow-on contract to finalize development, implementation, and program sustainment of the AWS Cloud-based operating environment. The CISA Office of the Chief Information Officer (OCIO) and the Chief Technical Officer are also working to secure various system technical approvals via the OCIO Change-Control Board and the Technical Reference Model, and CISA anticipates completing these approvals by April 2022. Once these approvals are received, CISA can begin initiating technical deployments to include data visualization capabilities, the data warehouse, NCCAD data feed, incident data feed, and the uploading of spreadsheets that contain a wide range of C-IED programmatic data. These actions are scheduled to be completed and reach Initial Operational Capability by March 2023. ECD: March 31, 2023.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix B
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, Office of Strategy, Policy, and Plans
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
CWMD Component 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