# Countering Improvised Explosive Devices Implementation Directive Manual


## Department of Homeland Security
## Cybersecurity and Infrastructure Security Agency
## Directive Manual Number: 6200-01
## Issue Date: 02/20/2024

# Table of Contents

# I. General Information

## A. Purpose

This Directive Manual (DM) establishes the Cybersecurity and Infrastructure Security Agency (CISA) Countering Improvised Explosive Devices (C-IED) Program to implement requirements of Presidential Policy Directive (PPD) 17, "Countering Improvised Explosive Devices," and its associated national plans.

## B. Scope of Application

This DM applies to all CISA employees, contractors, and detailees involved in CISA's C-IED Program.

## C. Exemptions

There are no exemptions to this policy.

## D. Supersession

None.

E. **Review Dates**

**This section is completed by SPP.**

1. Last Review Date: 02/20/2024
2. Effective Date: N/A
3. Next Review Date: 02/20/2027

F. **Revision Log**

**This section is completed by SPP.**

| Revised Section Number and Title | Deleted Section Number and Title | Approved By: | Date: |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |

## II. Responsibilities

A. The **Director, CISA**:
1. Establishes the CISA C-IED Program through this policy;
2. Assures effective implementation of national and Department of Homeland Security (DHS) C-IED requirements on CISA;
3. Resolves any compliance, interagency, or jurisdictional issues when needed; and
4. Serves as the national coordinator for the critical infrastructure security mission, coordinating with other sector risk management agencies to develop a national plan to secure critical infrastructure against cyber and physical threats to include Improvised Explosive Devices (IEDs).

B. The **Executive Assistant Director (EAD), Infrastructure Security Division (ISD)**:
1. Oversees and administers the various elements of the C-IED program and its operations falling under ISD;
2. Revises and issues implementing standards and procedures for this policy;
3. Oversees establishment of compliance and enforcement procedures for this policy; and
4. Synchronizes program elements across CISA, and resolves any compliance and cross-CISA, interagency, or jurisdictional issues that may arise, in coordination with the CISA Director when needed.

C. The **EAD, Cybersecurity Division (CSD)**:
1. Provides cybersecurity and technology subject matter expertise and technical guidance to secure C-IED technologies and enhance detection, mitigation, and response to their use for disruption; and
2. Understands, mitigates, and reports the threat of bomb-making information accessible online that can be misused to create IEDs that threaten life or infrastructure to the CISA Office for Bombing Prevention[1] (OBP) within CISA.

D. The **Heads of Divisions**:
1. Assure compliance with the requirements of this DM within their organizations;
2. Support implementation of national and DHS C-IED plans as required, in alignment with their missions while incorporating appropriate resources in their operating plans; and
3. Provide timely reporting on milestones, as required.

1. Approved and authorized branding of the Bombing Prevention Subdivision in ISD as the Office for Bombing Prevention (OBP) for public use. The branding was approved by CISA's Office of External Affairs in the memorandum, "Sub-Brand Justification for the CISA Office for Bombing Prevention," effective April 14, 2021.

E. The **Associate Director, Bombing Prevention, ISD**:
   1. Manages the CISA sub-division serving as the CISA OBP to build C-IED capabilities within the general public and across the public and private sectors to prevent, protect against, respond to, and mitigate bombing incidents;
   2. Coordinates the operational implementation of the DHS and CISA C-IED programs;
   3. Serves as CISA's formally designated representative on national and DHS C-IED planning and coordination bodies and performs the required duties therein; and
   4. Initiates, modifies, expands, and/or discontinues programmatic efforts as needed to maintain alignment with administration, legislative, and departmental guidance and informed by C-IED risk analysis to maximize program effectiveness and return on investment.

F. The **Associate Director, Chemical Security, ISD**:
   1. Ensures programs are in place to support chemical facilities risk management to prevent:
      a. An intentional onsite release of chemicals of interest (COI);
      b. A misappropriation of COI usable in an offsite attack; and
   2. Participates in C-IED planning and coordinates bodies involved in the program.

## III. Standards and Procedures

A. Description

1. CISA is required by legislation, executive mandate, and DHS policy to play a lead role in the national C-IED effort PPD-17, "Countering Improvised Explosive Devices," and its most recent applicable associated Implementation Plan (IPlan). PPD-17 re-established federal policy to develop, implement, and strengthen measures to prevent, protect against, respond to, recover from, and mitigate attacks using IEDs and their consequences at home and abroad.
2. The IPlan specifically requires CISA to coordinate public and private sector outreach and assistance programs to distinguish responsibilities, clarify scope, collaborate and/or deconflict program activities, share resources, and unify national messaging that avoids duplication and maximizes impact of C-IED programs to reduce the risk posed by IEDs.
3. The standards and procedures in this DM establish the coordinating and implementing functions and activities required of CISA to assure the agency's compliance with national and DHS policy and planning requirements.
4. The C-IED Program established by CISA implements C-IED strategies and policies that safeguard national infrastructure and the public through the agency's collaboration with all levels of government and private sector. Program elements consist of:
    a. National and DHS Coordination:
        i. The Associate Director of Bombing Prevention administers C-IED programs, including service as the Deputy Administrator of the Joint Program Office for Countering Improvised Explosive Devices (JPO C-IED) and chairs the DHS Improvised Explosive Device Working Group (IEDWG).
        ii. The Associate Director of Bombing Prevention serves as co-lead of the EU-US Explosives Experts Seminar and as CISA's formally designated representative to the First Responder Resource Group, the National Bomb Squad Commanders Advisory Board, and the International Association of Bomb Technicians among others.
        iii. Applicable CISA heads of divisions provide timely reporting on milestones through JPO C-IED and DHS IEDWG channels.
    b. Capacity Building, including:
        i. Information sharing;
        ii. Technical assistance;
        iii. Training and awareness;
        iv. Technology application and integration;
        v. Capability assessments and reporting; and
        vi. Other functions or activities that national and DHS plans require.
5. For additional information or questions, please contact (b) (6) [redacted].

B. National and DHS Policy, Planning, and Implementation Coordination

1. JPO C-IED
    a. The Associate Director of Bombing Prevention or designee, as CISA's designated representative, serves as the Deputy Administrator of this Program Office.
    b. The Deputy Administrator facilitates and assists the Joint Program Office (JPO) Administrator with executing the mission of the JPO C-IED by:
        i. Assisting in the coordination of meeting activities, which includes:
            1) Identifying items for and confirming meeting agendas with JPO C-IED staff;
            2) Incorporating agenda items and recommendations from JPO C-IED members and circulating correspondence as appropriate;
            3) Confirming interagency participation in meetings;
            4) Confirming DHS components, including CISA subject matter experts (SMEs) from CISA divisions, participating in meetings; and
            5) When required, soliciting executive-level coordination or participation and deconfliction from all relevant agencies.
        ii. Leading and facilitating the JPO C-IED Implementation Committee and its functional area working groups;
        iii. Managing and ensuring the implementation and maintenance of the national C-IED IPlan;
        iv. Monitoring the status of actions in the IPlan Appendix B, "Plans of Action" milestones on a quarterly basis;
        v. Leveraging milestone tracking to inform agency and department leadership of progress in C-IED efforts; and
        vi. Soliciting and assigning, as necessary, SMEs to participate in efforts that support the national C-IED mission.
2. DHS IEDWG
    a. CISA, by DHS policy, is the executive agent for the DHS IEDWG;
    b. The Associate Director of Bombing Prevention manages and chairs the DHS IEDWG as CISA's designated representative and is responsible for:
        i. Scheduling and convening meetings;
        ii. Facilitating development and publication of DHS action plan to meet the department's commitments to the national IPlan;
        iii. Escalating non-participation of component SMEs that impacts DHS execution of national IPlan through existing departmental lines of authority to encourage active participation in C-IED efforts;
        iv. Establishing process and metrics for status reporting, executed in alignment with JPO C-IED processes;
        v. Coordinating across DHS to develop and maintain strategic partnerships to implement DHS actions;
        vi. Soliciting and assigning, as necessary, SMEs across CISA divisions to participate in efforts that support DHS commitments when needed; and
        vii. Monitoring the status of DHS component commitments and milestones on a quarterly basis, and reporting results by:
            1) Issuing data calls quarterly to relevant DHS components via the CISA and DHS tasking system;

2) Developing a status report to contain progress updates on DHS-assigned elements of national C-IED policy implementation, where received, and identifying areas where non-participation is impacting tracking and/or execution of efforts;
3) Transmitting a report to the EAD of ISD;
4) Annually, compiling a status report and transmitting to the CISA Director, the heads of relevant DHS components with C-IED requirements under the national IPlans and the Office of the Secretary; and
5) Escalating to the EAD of ISD when reporting metrics that indicate non-compliance for intra-agency resolution and deconfliction, coordinating with the Director as needed.

C. Capacity Building

1. The OBP leads, coordinates, and executes C-IED Information Sharing requirements for CISA by:
   a. Establishing, maintaining, and operating the central and shared knowledge repository, the Technical Resource for Incident Prevention (TRIP*wire*), on counter-IED programs, activities, accomplishments, and products;
   b. Establishing, maintaining, and operating the National C-IED Capabilities Analysis Database to track, analyze, and report on both threat level and readiness information; measuring national, state, and jurisdictional preparedness and unit level capability; analyzing multiple levels of threat and preparedness data; and identifying previously unidentified preparedness gaps and data trends;
   c. Developing, standardizing, and sharing proven force protection and critical infrastructure protection measures across the C-IED community;
   d. Distributing information to appropriate private sector, public sector, and first responder stakeholders via CISA-established channels as well as its own developed C-IED community channels; and
   e. Working with Department of Justice and DHS Science and Technology to enhance global collaboration and international sharing of best practices to develop and implement voluntary measures between nations to better control the movement of IED precursor channels.
2. The OBP leads stakeholder IED preparedness by developing and providing a diverse curricula of nationally accredited counter-IED and risk mitigation training and awareness programs and resources to build relevant core capabilities and enhance awareness of IED threats among state, local, tribal, and territorial private sector partners, and the general public.
3. The OBP delivers tailored assistance to communities to improve their C-IED capabilities by providing or coordinating the deliberate application of the OBP's resources and services to stakeholders, and investment into communities across the nation.
4. Chemical Security within ISD implements its responsibilities to the IPlans by:
   a. The Associate Chief or designee serving as a contributing representive along with CISA's formally designated representative on national and DHS C-IED planning

and coordinating bodies and performing the required duties required as a representative;

b. Supporting development, production, and distribution of information and programs to reduce the risk associated with explosive precursor COI's used to manufacture homemade explosives and produce IEDs and other relevant actions as required by the IPlans.

5. CSD provides cybersecurity, technology subject matter expertise, and technical guidance, and takes actions to support CISA's C-IED Program by:
   a. Providing stakeholder guidance to:
      i. Secure C-IED technologies from cybersecurity vulnerabilities; and
      ii. Enhance detection, assessment, and response to technologies (i.e., bot farms) designed to generate web enabled serial bomb threats or amplification of threats/incidents to a mass scale for disruptive purposes.
   b. Understanding, mitigating, and reporting the threat of bomb-making information accessible online that can be misused to create IEDs that threaten life or infrastructure.
6. The OBP develops, implements, and executes C-IED Capability Assessments which collect and analyze information regarding community preparedness to counter IEDs.
   a. These assessments incorporate information from the state, local, and unit level which develops a complete, accurate, and comprehensive picture of the nation's C-IED capabilities.
   b. Assessment activities consist of data collection and validation, data access and management, and data assessment, analysis, and dissemination.
7. The OBP fosters technology solutions that can address identified C-IED capability gaps to strengthen the security and resilience of the C-IED critical infrastructure community and the individual bomb technician. The OBP accomplishes this by:
   a. Coordinating with private sector partners to identify emerging technologies that can help address the risk from IEDs; and
   b. Strengthening the coordination of federal government research, development, test, and evaluation activities relating to the detection, prevention of, protection against, and response to IED attacks and isolation of and rendering safe of IEDs.

D. Compliance and Enforcement

1. Consequences for Noncompliance:
   a. Noncompliance with this policy leads to insufficient fulfillment of CISA's role in national C-IED policy, which may damage the agency's reputation and diminish trust from interagency stakeholders within the C-IED prevention mission; and
   b. Insufficient attention to C-IED prevention and protection measures increases the risk of a bombing incident occurring, potentially harming national infrastructure, and life.
2. Compliance Procedures and Enforcement Methods:
   a. Internal reporting to senior leadership, such as in ISD's quarterly division Management Reviews, for enforcement and clear deliverables and objectives,

congruent with the national and DHS IPlans/policies are incorporated into the division's Annual Operating Plan and program plans.

b. Other enforcement and compliance procedures have been incorporated into the implementation standards and procedures of the policy.

## IV. Authorities

A. Public Law (Pub. L.) 115-278, "Cybersecurity and Infrastructure Security Act of 2018"
B. Pub. L. 109-295, "Department of Homeland Security Appropriations Act, 2007"
C. 6 United States Code (U.S.C.) 652, "Cybersecurity and Infrastructure Security Agency"
D. 6 U.S.C. 654, "Infrastructure Security Division"
E. PPD 17, "Countering Improvised Explosive Devices"
F. PPD 21, "Critical Infrastructure Security and Resilience"
G. Homeland Security Presidential Directive 19, "Combating Terrorist Use of Explosives in the United States"
H. Emergency Support Function 14, "Cross-Sector Business and Infrastructure"
I. DHS Decision Memorandum, "Establishment of DHS Improvised Explosive Device Working Group"
J. Charter of the Joint Program Office for Countering Improvised Explosive Devices (IEDs) (JPO C-IED)
K. Countering Improvised Explosive Devices Implementation Plan, May 10, 2019
L. Countering Improvised Explosive Devices Implementation Plan Plans of Action, September 11, 2020

## V. Signature

(b) (6)

Jen Easterly, Director
Cybersecurity and Infrastructure Security Agency

02/20/2024
Date

## Appendix A:
## References

I. DHS Memorandum for Distribution, "Establishment of DHS Improvised Explosive Device Working Group," February 28, 2007.[2]
II. CISA Memorandum for Distribution, "Sub-Brand Justification for the CISA Office for Bombing Prevention," April 14, 2021.[3]

2. A copy of this document may be obtained upon request from ISD OBP at (b) (6)
3. A copy of this document may be obtained upon request from ISD OBP at

## Appendix B:
## Definitions and Acronyms

A. **Definitions**

1. **Chemicals of Interest (COI)**: Chemicals considered to pose risks based on release, theft or diversion, or sabotage.

2. **Countering Improvised Explosive Devices (C-IED)**: The interdisciplinary processes for developing, implementing, evaluating, and adjusting measures to prevent, discover, protect against, mitigate, respond to, and recover from IED incidents and their consequences.

3. **Department of Homeland Security Improvised Explosive Device Working Group (DHS IEDWG)**: Working group established to coordinate programs and improve capabilities to prevent domestic terrorist bombing attacks with the following goals:
   a. Establish a common understanding of roles and responsibilities among DHS components with respect to bombing prevention;
   b. Assist CISA in fulfilling its congressional mandate[4] to coordinate national and intergovernmental bombing prevention activities by providing a unified and consistent voice for DHS;
   c. Inventory and assess the sufficiency of current DHS bombing prevention programs;
   d. Articulate the DHS position, role, and leadership in national bombing prevention and response to the nation; and
   e. Aid in development and implementation of the National Strategy for Bombing Prevention.

4. **EU-US Explosives Experts Seminar**: The EU-US Experts Seminar focuses on European Union and United States initiatives that impact explosive policy, homemade explosives and precursors, new trends and tactics, techniques and procedures, detection of explosives, explosives detection canines, explosives related training, aviation security, small unmanned aircraft system threats and counter unmanned aircrafy system considerations, information sharing, and case studies. The EU-US Experts Seminar and follow-on discussions support and reaffirm the important role that CISA/ISD plays in mitigating the risk of IEDs and associated precursor chemicals.

5. **First Responder Resource Group (FRRG)**: The DHS Science and Technology Directorate's (S&T) FRRG is an all-volunteer working group that helps S&T maintain focus on the top-priority needs of responders in the field. Members represent a broad range of disciplines (law enforcement, fire service, emergency medical service, emergency management, and more), sectors (local, state, tribal, and federal

4. DHS Decision Memorandum, "Establishment of DHS Improvised Explosive Device Working Group."

government), as well as first responder professional associations and geographic regions. The FRRG's primary role is two-fold: (1) identify high-priority capability gaps in the first responder community that S&T development efforts might be able to fill; and (2) define operational requirements that technologies and knowledge products must meet in order to effectively fill those gaps. FRRG members also often help validate and evaluate solutions during development.

6. **Improvised Explosive Device (IED)**: A device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals designed to destroy, incapacitate, harass, or distract. It may incorporate military stores but is normally devised from non-military components. Refers to a type of IED incident that involves a complete functioning device.

7. **International Association of Bomb Technicians and Investigators (IABTI)**: The IABTI is an independent, non-profit, professional association formed for countering the criminal use of explosives. This is sought through the exchange of training, expertise, and information among personnel employed in the fields of law enforcement, fire and emergency services, the military, forensic science, and other related fields.

8. **Joint Program Office for Countering Improvised Explosive Devices (JPO C-IED)**: An interagency entity chartered under the authority of the United States Attorney General with the Federal Bureau of Investigation as its executive agent, which facilitates the integration and alignment of domestic, transborder, and international activities across the United States government necessary to counter IEDs in accordance with national policy. The JPO C-IED improves interagency coordination, reduces duplication of efforts, and systematically eliminates gaps in national security posture that could be exploited by terrorists or other criminals. The JPO C-IED coordinates, tracks, and as necessary, escalates implementation issues relating to the execution of specific tasks to counter the use of IEDs. The JPO C-IED provides for the resolution of identified policy and implementation issues by the National Security Council, as needed.

9. **JPO C-IED Administrator**: Administrator, appointed by the JPO C-IED Senior Executive, who: 1) Organizes, directs, and manages the functions of the JPO C-IED staff and all assigned resources thereof; 2) Provides JPO C-IED program review and milestone information to the Executive Council; 3) Represents the JPO C-IED mission to the private sector and international partners, as appropriate; 4) Performs other duties as directed by the Executive Council; and 5) Facilitates monthly JPO C-IED Implementation Committee meetings.

10. **JPO C-IED Implementation Committee**: An interagency committee operating an element of the JPO C-IED. It reflects the joint counterterrorism, diplomatic, homeland security, intelligence, law enforcement, military, and public safety disciplines necessary to coordinate federal activities and engage with state, local,

tribal, and territorial governments, and international and private sector partners, to counter IEDs.

11. **National Bomb Squad Commanders Advisory Board (NBSCAB)**: The NBSCAB serves as the leadership element for Public Safety Bomb Squads, provides advice to federal agencies in direct support of important bomb squad related issues and functions as a decision making authority for recommended guidelines and standards for the profession. The NBSCAB is made up of 12 voting members who are elected by their peers. The NSCAB meets a minimum of three times yearly.

12. **National C-IED Capabilities Analysis Database**: National C-IED Capabilities Analysis Database is a national C-IED data and analytical information technology system that incorporates and synthesizes C-IED data from various internal and external sources to enable users to track, analyze, and report on both threat level and readiness information; measure national, state, and jurisdictional preparedness and unit level capability; analyze multiple levels of threat and preparedness data; and identify previously unidentified preparedness gaps and data trends.

13. **Office for Bombing Prevention (OBP)**: The organization which leads DHS efforts to implement the nation's C-IED policy and enhance the nation's ability to prevent, protect against, respond to, and mitigate the use of explosives against life; critical infrastructure; the private sector; and federal, state, local, tribal, and territorial entities.

14. **Sector Risk Management Agency**: A federal department or agency, designated by law or presidential directive, with responsibility for providing institutional knowledge and specialized expertise of a sector, as well as leading, facilitating, or supporting programs and associated activities of its designated critical infrastructure sector in the all-hazards environment in coordination with DHS.

15. **Technical Resource for Incident Prevention (TRIP*wire*)**: The Technical Resource for Incident Prevention, TRIP*wire*, is a collaborative, online information and resource sharing portal for the nation's security and emergency services professionals. TRIP*wire* raises awareness of evolving IED tactics, techniques, and procedures, as well as incident lessons learned and counter-IED preparedness information.

B. **Acronyms**

| Acronyms | |
|---|---|
| C-IED | Countering Improvised Explosive Device |
| CISA | Cybersecurity and Infrastructure Security Agency |
| COI | Chemical of Interest |
| CSD | Cybersecurity Division |

| | |
|---|---|
| DHS | Department of Homeland Security |
| DM | Directive Manual |
| EAD | Executive Assistant Director |
| FRRG | First Responder Resource Group |
| IABTI | International Association of Bomb Technicians and Investigators |
| IED | Improvised Explosive Device |
| IEDWG | Improvised Explosive Device Working Group |
| IPlan | Implementation Plan |
| ISD | Infrastructure Security Division |
| JPO | Joint Program Office |
| JPO C-IED | Joint Program Office for Countering Improvised Explosive Devices |
| NBSCAB | National Bomb Squad Commanders Advisory Board |
| OBP | Office for Bombing Prevention |
| PPD | Presidential Policy Directive |
| Pub. L. | Public Law |
| SME | Subject Matter Expert |
| S&T | Science and Technology Directorate |
| TRIP*wire* | Technical Resource for Incident Prevention |
| U.S.C. | United States Code |