OFFICE FOR BOMBING PREVENTION

Bombing Prevention Resources for Mitigating the Use of Explosives and IEDs Against Critical Infrastructure

Homeland Defense & Security Information Analysis Center (HDIAC) Webinar

Agenda

1 Threat Overview

2 Office for Bombing Prevention (OBP) Focus Areas

3 Awareness Products

4 Guidance & Key Tips

5. Closing

Threat Overview

Terrorism Risk Landscape: Improvised Explosive Devices (IEDs)

Terrorist groups continue to advocate for attacks that use IEDs in several different ways:

- ☑ **Inspire** homegrown IED attacks outside of conflict **zones through social media**

- ☑ Raise domestic violent extremism, including religiously, racially, and politically motivated violence

- ☑ **Use homemade explosives (HMEs) in IED attacks** by both domestic and foreign terrorist organization (FTO)-inspired threat actors

- ☑ **Strike aviation and transportation hubs** with concealed IEDs, as well as other key critical infrastructure sectors

- ☑ **Attach explosives to unmanned aircraft systems (UASs) to target critical infrastructure**, soft targets, and crowded, open-air venues
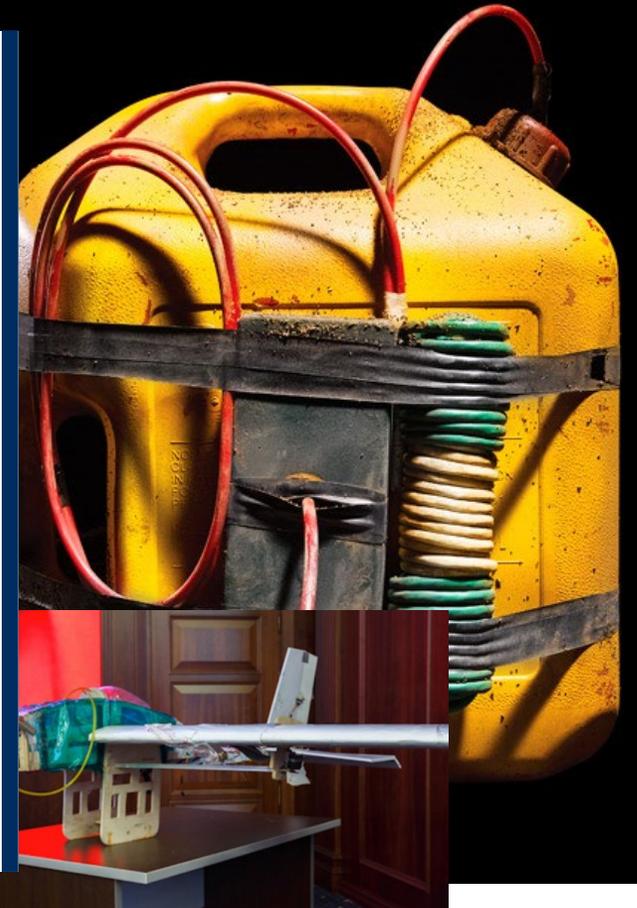
Domestic IED Threats

The IED threat to the United States continues to come from a wide variety of different individuals, groups, and ideologies. Among the serious threats is domestic, violent extremism.

Transnational Organized Crime

Domestic Terrorists/HVEs

Foreign Terrorist Organizations

Idiosyncratic Individuals

Domestic IED Threats

Juveniles & Hobbyists
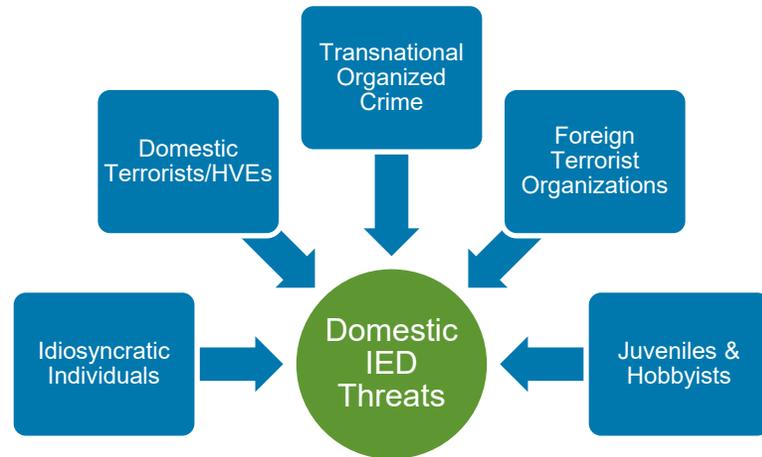
- **Collaboration** between criminal and terrorist networks occurs at home and overseas.

- **Practical instructions** on IED construction and concealment techniques proliferate throughout the **internet and social media.**

- IED components, explosives, and HME **precursors are readily available** in the United States.

- IED construction and deployment techniques **continue to evolve and proliferate** toward multiple attack scenarios.

Notable Incidents

Timothy McVeigh – Oklahoma City
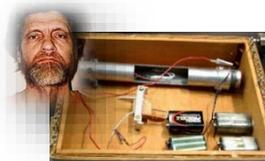
Ted Kaczynski – Unabomber

Eric Rudolph– Centennial Olympic Park Bomber

Kevin Harpham – MLK Memorial March

Mark Conditt – Austin, TX, Package Bomber

Anthony Quinn Warner – Nashville VBIED Attack

Domestic IED Threat Analysis - 2021

2021 AT A GLANCE

Total open-source intelligence IED incident numbers increased to (2,139) in 2021 from (2,061) in 2020.

- ↑ **39% Bomb Threats:** The steep increase in bomb threats from (687) in 2020 to (954) incidents in 2021 was likely the result of schools reopening post-COVID-19 pandemic.

- ↑ **18% Suspicious Packages:** The rise in the number of suspicious package incidents from (400) in 2020 to (470) in 2021 was likely the result of the nationwide reopening of the economy post-COVID-19 pandemic.

- ↓ **27% Device-Related Incidents:** The total number of device-related incidents (715) declined in 2021 from (786) in 2019 and (974) in 2020. The increase in 2020 was a deviation from the 3-year averages due to the increased use of explosive devices used during the nationwide civil unrest that began in May 2020.

Source: TRIP*wire*

2021 National Overview
Total: 2,139 incidents

Region	Incidents
Region 1	130
Region 2	154
Region 3	258
Region 4	425
Region 5	349
Region 6	216
Region 7	96
Region 8	100
Region 9	296
Region 10	115

19 Killed
120 Injured
675 Arrested

Count	Category
246	Device Functioned
12	Device Emplaced
405	Device Discovered
52	Bomb-Making Material
470	Suspicious Package
954	Bomb Threat
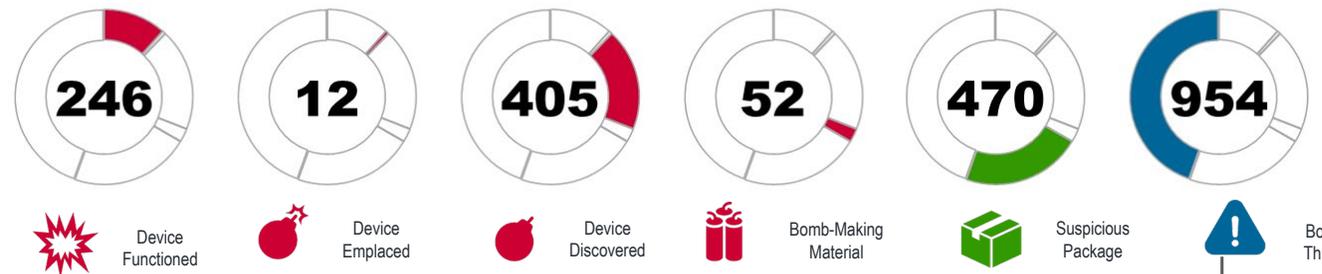
2021 Domestic, Violent Extremists Attacks and Plots Increase

Many protests in 2021 were marred by violence by actors from across the political spectrum who sought to exploit social and political divisions. Protests over police violence and subsequent violent counter-protests continued to be a major source of concern for law enforcement officers. Federal, state, and local government buildings were the most frequent targets for the devices discovered or used during anti-government protests.

Source: www.portlandoregon.gov

31 December 2020 - 1 January 2021
Violent rioters in a crowd of 80-100 individuals launched at least 2 improvised incendiary devices (IIDs), described as Molotov cocktail-style devices, and commercial-grade aerial pyrotechnics at the Federal Courthouse and Justice Center in downtown Portland.

Source: al.com

6 January 2021
Authorities found 11 IIDs, described as Molotov cocktails, in the truck of a 70-year-old Alabama man arrested during the riots at the U.S. Capitol Building. The IIDs were made of mason jars filled with gasoline and Styrofoam, with golf tees and rags for fuses.

Source: Al.com/

Source: abcnews.go.com/

21 January 2021
A 25-year-old man arrested for breaking windows at the Democratic Party of Oregon office was found to have 4 Molotov cocktails in his backpack. The IIDs were made of green beer bottles wrapped in socks with cloth wicks.

Source: Trendsmap.com/

Source: WDBJ7.com/

29 June 2021
FBI agents searched the Virginia home of a former Rocky Mount Police officer who had been arrested for his role in the riots at the U.S. Capitol. During the search, the FBI discovered a partially assembled pipe bomb.

Source: WDBJ7.com/

Bomb Threats Against Academic Institutions

Recent bomb threats at Historically Black Colleges and Universities (HBCUs) and Ivy League Universities have increased the need for bombing prevention training and awareness products.

- Increase in bomb threats against Ivy League Schools in November 2021 due to bomb threat campaign.

- Greater-than-normal frequency of bomb threats against HBCUs in January and February 2022.

- Most bomb threats were harmless and perpetrated by students without malicious intent to harm others.

- Numerous studies show direct bomb threats rarely involve an actual device. Data from the ATF shows that from 1990 to 2002, of 1055 identified explosives-related incidents at schools, only 14 (1.3%) were preceded by a bomb threat.

- **There is almost no motivation for someone who wants to target a school to alert authorities before hand.**

Bomb Threats Targeting HBCUs in 2022

OBP Instructor Rich Knight Teaches Bomb Threat Management to HBCU Stakeholders

EAD, Dr. David Mussington With AUCC Executive Director, Dr. Michael Hodge at a Bomb Threat Forum for HBCUs

Mass Bomb Threat Awareness Job Aid Provided to HBCUs

CISA Critical Resources for Handling Bomb Threats Video Served as Another Resource for HBCU Leadership

HBCU Threat

- January and February of 2022 saw a wave of bomb threats targeting HBCUs

  - More than 30 of the 101 HBCUs received bomb threats

  - Over 70 bomb threats were reported against HBCUs and other minority institutions nationwide in January and February 2022

- OBP responded by providing resources and training opportunities both in person and virtually nationwide.

Emerging Threat: Weaponized UASs

The ability to attach explosives to UASs raises the concern that threat actors may use the TTP to target critical infrastructure, soft targets, and crowded, open-air venues.
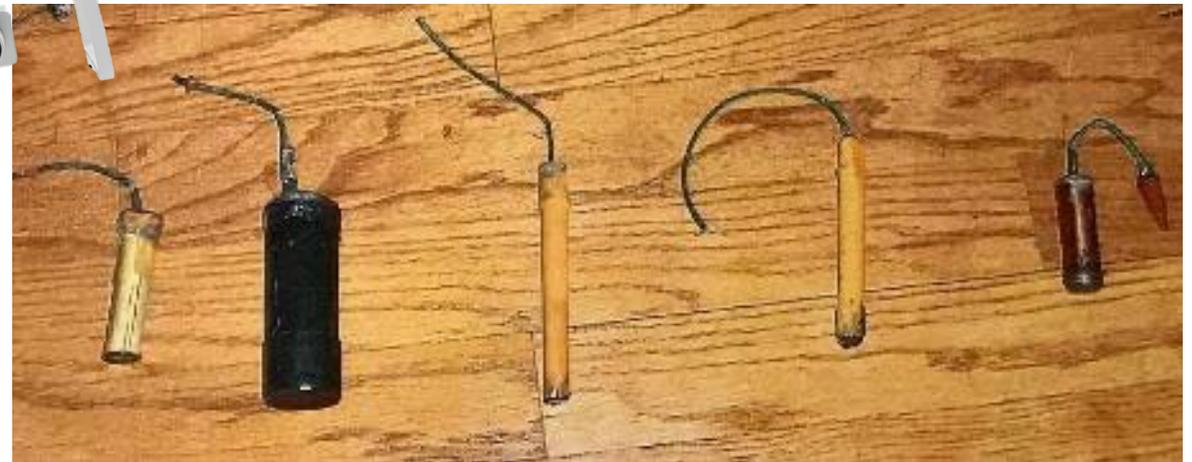
Surveillance footage capturing 2019 PA incident; UAS utilized; and devices collected from the suspect's residence

Office for Bombing Prevention (OBP) Focus Areas

Mission and Focus Areas

CISA OBP accomplishes its mission through a portfolio of complementary counter-IED (C-IED) services.

CISA OBP leads Department of Homeland Security (DHS) efforts to implement National C-IED policy and enhance the nation's ability to prevent, protect against, respond to, and mitigate the use of explosives against critical infrastructure; the private sector; and federal, state, local, tribal, and territorial entities.

Training & Awareness

- In-person, Instructor-Led, In-resident, and Mobile Training
- Online Distance Learning - Virtual Instructor-Led Trainings and Web-Based Independent Studies
- Learning Solutions Curriculum and Awareness Product Design and Development
- Train-the-Trainer Capability and Capacity Building

Policy Coordination

- Policy Design and Coordination
- Communications and Outreach
- C-IED Guidance and Product Design

Information Sharing

- TRIP*wire*
- C-IED and IED Information Sharing
- IED Incident and Threat Reporting
- Intra-agency Intelligence Coordination

Technical Assistance & Services

- C-IED Capability Assessments
- CI/Special Event Planning
- Explosive Blast Modeling
- C-IED Technology Development and Evaluation
- C-IED Grant Requirements Support
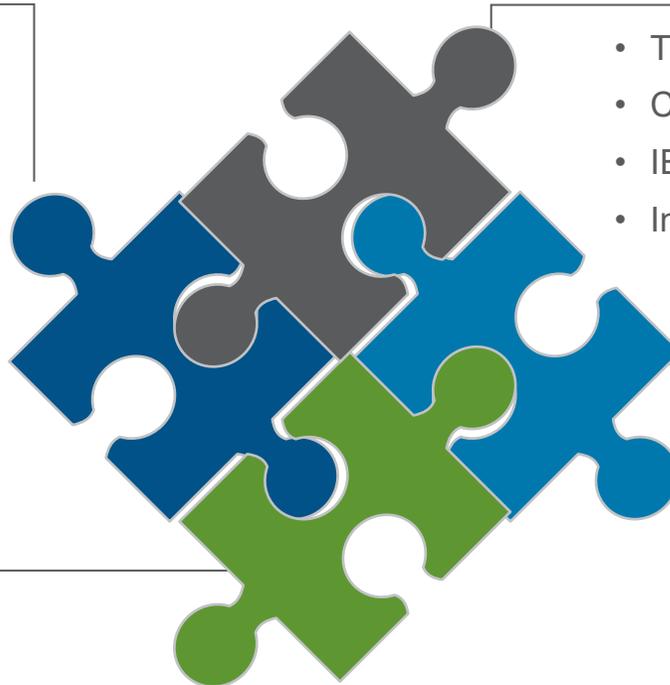
C-IED Training Overview

CISA OBP delivers a diverse curriculum of accredited training to build nationwide C-IED awareness and capabilities among stakeholders.

Diverse Curriculum

Diverse curriculum of nationally accredited training designed to build counter-IED core capabilities, such as

- IED Awareness
- Suspicious Items/Activity
- Bomb Threat Management
- Protective Measures

Participants

- State and Local Law Enforcement
- Federal Agencies
- First Responders and Receivers
- Private Sector Partners

Access Training

- In-Person, Instructor-Led Training – 9 courses
- Virtual Instructor-Led Training – 6 courses
- Web-Based Training – 5 courses

Access courses at cisa.gov/bombing-prevention-training-courses

C-IED Training Courses

CISA OBP offers training to build C-IED capabilities through a variety of modalities to meet different stakeholders' needs.

In-Person

- Bombing Prevention Awareness
- Bomb Threat Management Planning
- IED Search Procedures
- Protective Measures
- Surveillance Detection
- Vehicle-Borne, Improvised Explosive Device Detection
- Bomb-making Materials Awareness Program (BMAP) Community Liaisons

Virtual Instructor

- IED Construction and Classification
- IED Explosive Effects Mitigation
- Introduction to the Terrorist Attack Cycle
- HMEs and Precursor Awareness
- Protective Measures Awareness
- Response to Suspicious Behaviors and Items

Self-paced Independent Study Training

- IED Awareness and Safety Procedures
- HMEs and Precursor Chemicals Awareness for Public Safety
- Bomb Threat Preparedness and Response
- Bomb-Making Materials Awareness: Your Role
- Bomb-Making Materials Awareness Employee Training

TRIP*wire*

Program Overview and Outcomes

- Secure website for IED incident information, tactical trends, lessons learned, and comprehensive C-IED preparedness and risk management information to **raise awareness and empower stakeholders to fill capability gaps** (tripwire.dhs.gov).

- TRIP*wire* 2.0 offers features that provide a powerful user experience, including enhanced search functionality, an interactive domestic IED incident map, and password self-reset.

Increases awareness of evolving IED tactics, techniques, and procedures

Shares incident lessons learned and counter-IED preparedness information with security personnel

Integrates open-source information, including videos and how-to manuals gathered directly from extremist groups, to increase awareness of IED trends and threats

Publishes threat, awareness, and training materials to help first responders and law enforcement anticipate, identify, and prevent bombing incidents

Impacted Stakeholders

Public

Government

Private Sector

Law Enforcement

To register for an account, visit https://tripwire.dhs.gov

Phone: (866) 987-9473 | Email: TripWireHelp@dhs.gov

BMAP & Operation Flashpoint

BMAP

- BMAP is a counter-terrorism **risk management** bombing prevention program.

- Increases identification of **suspicious activity** and purchasing behavior by focusing on the acquisition of materials and bomb-building.

- Explosive precursor chemicals (EPCs) and other **bomb-making materials are so common that regulation alone is impractical**; at least 250K stores in the United States sell relevant products.

OPERATION FLASHPOINT

- "Operation Flashpoint" builds upon BMAP by **increasing the scale of business engagement through a field-based partnership with the FBI** Weapons of Mass Destruction Directorate.

- The Operation Flashpoint Pilot has been **implemented** in all 10 CISA regions as well as all 56 FBI field offices.

- **Finalize and enhance SAFETY Act block designations**, allowing the BMAP to be a qualified anti-terrorism technology (QATT).

'Report suspicious purchases': Feds kick off Operation Flashpoint, educating retailers who sell bomb-making materials
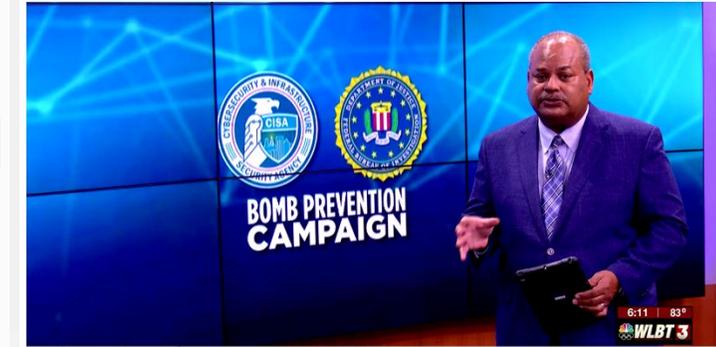
Cybersecurity and Infrastructure Security Agency @... · Jul 1
We launched a joint initiative with the @FBI to build awareness in communities across the U.S. for preventing bomb attacks. #OperationFlashpoint will help educate the public. Learn more: cisa.gov/news/2021/06/3...

Joint initiative across the U.S. for preventing bomb attacks.
OPERATION FLASHPOINT

Awareness Products

C-IED Awareness Products

CISA OBP offers a wide range of resources to share information and enhance C-IED preparedness, such as job aids, checklists, posters, cards, guidance, and videos.

Job Aids and Checklists

Informative quick-reference tools to support decision making in responding to bomb threats, suspicious activity/items, and terrorist/criminal threats.
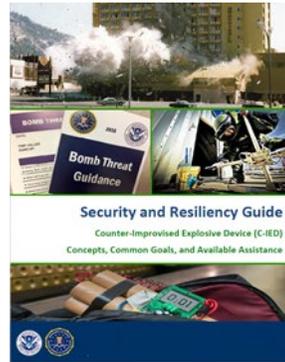
Bombing Prevention Guides

A source of counter-IED and risk management information and guidelines to help prevent, protect against, respond to, and mitigate explosive threats and bombing incidents in an orderly and controlled manner.

Awareness Posters and Cards

A variety of handy quick-reference cards and informative posters that prominently present key bombing prevention information in an easy-to-understand format. These cards and posters cover many counter-IED topics.
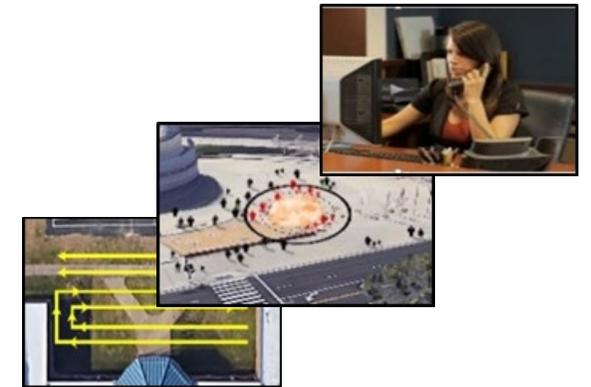
Videos

Instructional videos that communicate IED threats, explain counter-IED concepts, and demonstrate bombing prevention procedures by showing audiences how to react to a bombing attack and deal with a variety of explosive threats.

Available to the public at: cisa.gov/counter-ied-awareness-products

CISA OBP's Capability Building Framework

The *Security and Resiliency Guide for Countering IEDs* (SRG C-IED) serves as a foundational resource through which CISA OBP assists stakeholders to build C-IED capabilities.

The SRG C-IED provides stakeholders with access to:

- An overview of IED **threats** and **consequences**

- C-IED concepts and a set of **common C-IED goals**

- Links to federal government C-IED **tools** and **resources**

- Annexes for **high-risk** sports venues, public assembly venues, outdoor events, healthcare facilities, and lodging facilities

For more information, please visit cisa.gov/publication/security-and-resiliency-guide-and-annexes
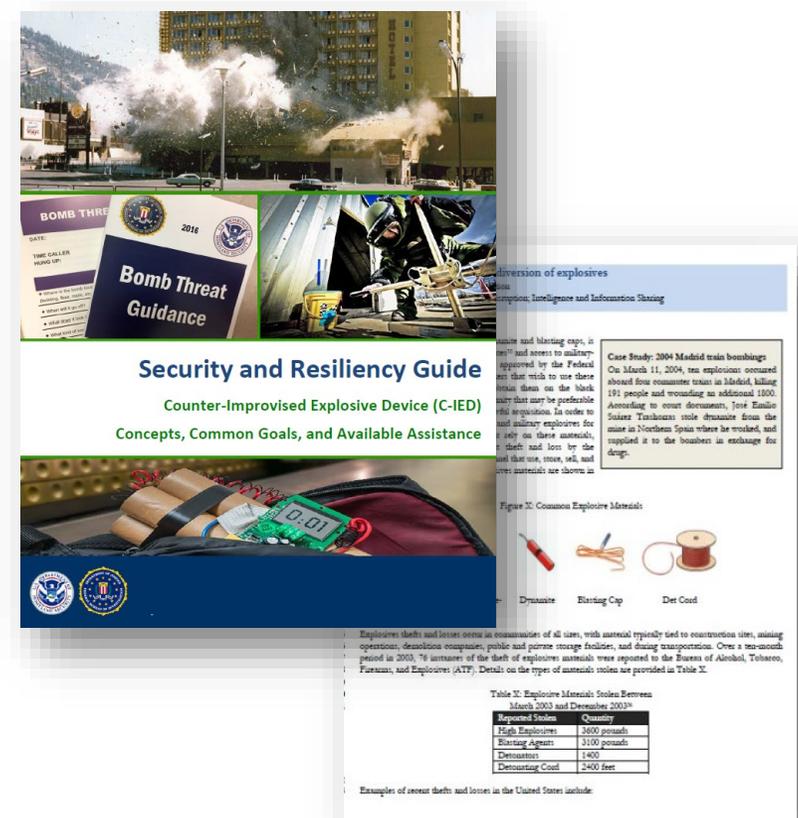
Guidance & Key Tips

Identifying IEDs

What is an IED?

An IED is "Any device **placed or fabricated** in an **improvised manner** incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and designed to destroy, incapacitate, harass, or distract."

Identifying the components of an IED

Use the acronym **SIMP-CE** to help remember the components of an IED:

Switch | **I**nitiator | **M**ain Charge | **P**ower Source — **C**ontainer | **E**nhancement

Assessing & Responding to a Bomb Threat

Determine whether the threat represents a Low, Medium, or High Risk, based on the Realism, Plausibility, Directness, and Immediacy/Eminence of the threat. Different threat levels correspond to different courses of action.

Low Risk: Lacks Realism
Threat is **vague, indirect,** and poses minimum risk to public safety. Probable motive is to cause **disruption.**
Assess & Lockdown (Partial or Full)

Medium Risk: Increased Realism
Threat could **feasibly be carried out**, but may not appear entirely realistic.
Threat indicated a **place, time, and possible steps taken** toward an attack.
Assess, Lockdown, & Search (Partial or Full)

Assess & Discount

Threat

High Risk: Specific and Realistic
Threat is **direct, specific, and realistic**; may include names, times, or locations.
Threat poses an **immediate and serious danger** to the safety of others.
*Assess & Evacuate (Partial or Full)*

Site Decision Maker or appropriate on-site supervisor ultimately determines what action to take, regardless of the assessment

Tips for Locating a Suspicious Item

Criminals or terrorists sometimes conceal IEDs in backpacks, suitcases, or common items. To determine if an item is suspicious or unattended, ask "Is the item HOT?"

Is it **HOT**?

Hidden
- Placed out of sight
- Appears purposely concealed

Obviously suspicious
- Unexplainable wires or electronics
- Bomb-like components

not Typical
- Out of place for the location
- Potentially related to a threat

- Use R. A. I. N. (Continue to other side)

YES (Suspicious)

NO (Unattended)
- Treat with caution
- Try to determine the owner
- Report to an authority
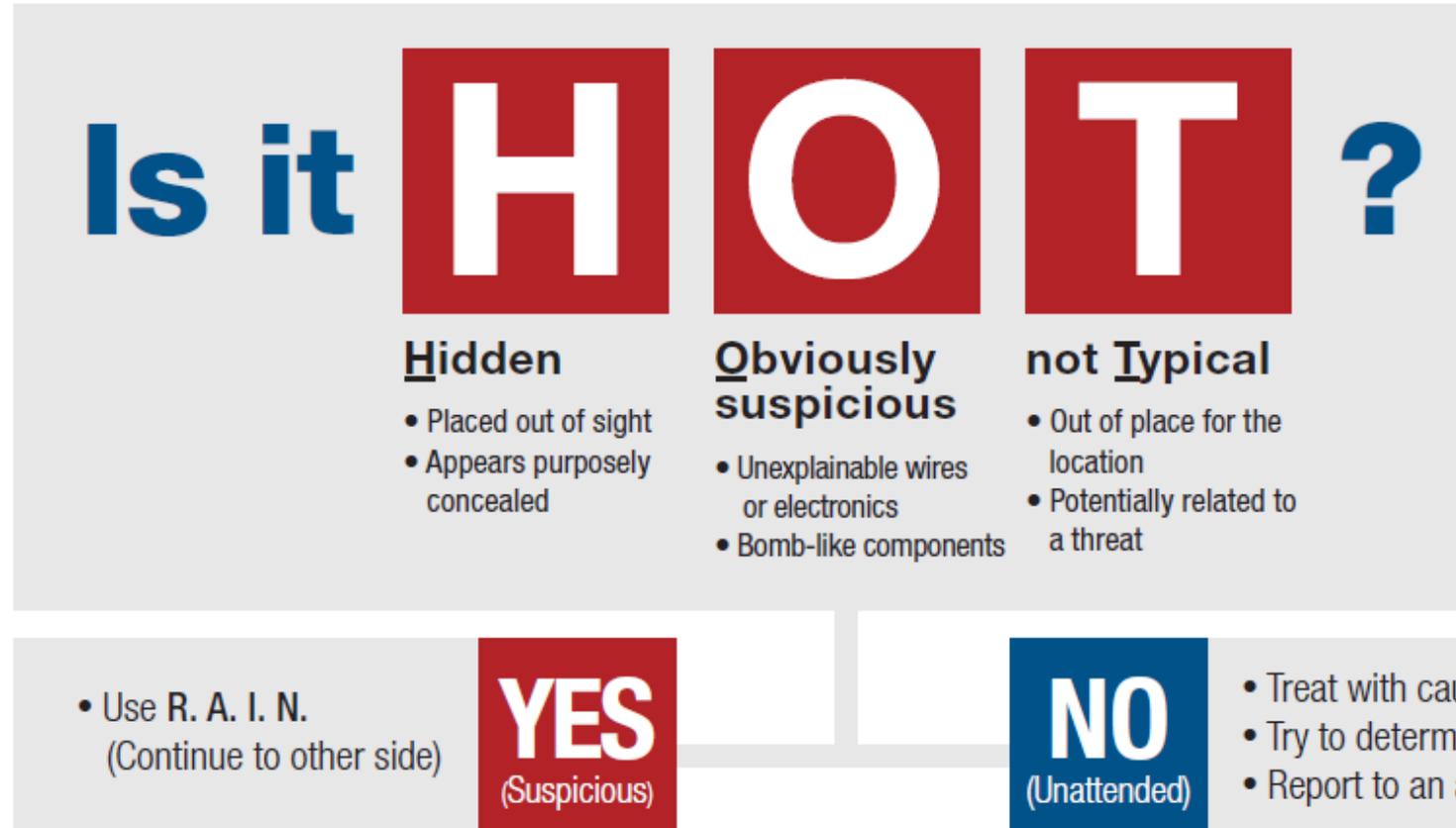
Best Practices When Encountering Suspicious Packages

When encountering a suspicious item, remember to R.A.I.N:

R — **Recognize the Indicators of a Suspected Explosive Device**

Indicators can be related to the characteristics, events, location, or time, including whether the item is Hidden, Obviously suspicious, or not Typical (HOT).

A — **Avoid the Area**

Don't touch the suspected item. Instead, immediately move and direct others to move away immediately.

I — **Isolate the Suspected Item**

Establish a perimeter to secure the area and continue to direct people away. Use frontal and overhead cover and if available wear personal protective equipment.

N — **Notify Appropriate Emergency Services**

Describe the **S**uspicious items and persons, the person's **A**ctions, the **L**ocation of the item, the **T**ime of placement and discovery, and **Y**our actions to mitigate risk (SALTY).

If you **see** something, **say** something®

REPORT SUSPICIOUS ITEMS. Contact **local law enforcement** or **9-1-1** in case of emergency

Closing

CISA OBP Contact Information

For questions or requests from specific programs, please reach out to the following:

Branch	Point of Contact
General Inquiries	General OBP Mailbox, obp@cisa.dhs.gov
Training Branch	Curt Tilley, Curtis.Tilley@cisa.dhs.gov Training Mailbox, OBPTraining@cisa.dhs.gov
Data & Analysis Branch	Will Byrd, William.Byrd@cisa.dhs.gov TRIPwire Mailbox, TRIPwireHelp@cisa.dhs.gov
Technical Assistance Branch	Darrin Flick, Darrin.Flick@cisa.dhs.gov Technical Assistance Mailbox, OBPCAP@cisa.dhs.gov
Strategy Branch	Doug DeLancey, Douglas.DeLancey@cisa.dhs.gov Strategy Mailbox, OBPCSICS@cisa.dhs.gov

For more information:
cisa.gov/obp

Questions?

OBP@cisa.dhs.gov
Jason.Stewart@cisa.dhs.gov