


From: Mike Sena msena@ncric.ca.gov 
Subject: Threat Coordination Call Notes - Electoral Vote in Congress to Inauguration Day, Washington DC
Date: January 4, 2021 at 2:43 PM
To:
Cc: Harvin, Donell (HSEMA) Donell.Harvin@dc.gov

MS

Dear Partner,

Thank you and your team for joining the call today with Donell Harvin and the NTIC team. As Washington DC prepares for the Electoral Vote in Congress on January 6, and the Inauguration of the President on January 20, the NTIC is working diligently to protect public safety, as well as privacy, civil rights and civil liberties. The NTIC has a collection requirement for individuals stating their intent to violate DC weapons laws and/or commit acts of violence at the upcoming major events in DC. The NTIC will be sending specific RFI's on subjects or groups that have been associated with planned criminal activity or [suspicious activity](#) through <https://rfi.dhs.gov> . Starting tomorrow, the NTIC will open a HSIN Connect room for the January 6 event. If you would like to join or have members of your team join the HSIN Connect room, please e-mail donell.harvin@dc.gov.

In the event of a major incident, threat information will be shared through the HSIN SitRoom: <https://share.dhs.gov/sitroom> . Please see the recommendations below for a fusion center's role during mass-casualty incidents and major events.

If a major cyber threat coincides with these planned events, personnel with the appropriate prior access permissions described below* may join: <https://share.dhs.gov/cyber> . Prior approval for access to the cyber room may be requested at CINaccess@nfcausa.org.

If a major incident requires a SitRep video teleconference call, we will use:

<https://ncric-ca-gov.zoomgov.com/j/1607386891?pwd=STRiUTd5ZU1OSDkyTHVuQXAxexFvZz09>

or +18335688864,,1607386891#,,0#,,89481052# (Toll-Free)
+16692545252,,1607386891#,,0#,,89481052# US (San Jose)
+16468287666,,1607386891#,,0#,,89481052# US (New York)

Below are the abbreviated notes of the questions and answers (Q&A) from today's call.

Q: Is there any information on planned violent counter-protestors attending the event?

A: The DC Mayor has asked counter-protestors to stay at home and many of the groups that have previously been involved in counter-protest activities have told their members not to come out due to safety concerns. NTIC suspects that the counter protesters will come out regardless. There is limited information on the potential for violent counter-protest activity.

Permitted events are planned at:

- [Freedom Plaza](#), 1/5 at 1pm Eastern.
- [The Ellipse](#), 1/6 at 9am Eastern.
- [Capitol Building \(North East Dr\)](#), 1/6 at 1 pm Eastern.

Q: What are the names of the groups advocating potential criminal or suspicious activity that were mentioned earlier that are confirmed or expected to attend?

A: Individual group names will be shared via HSIN Exchange.

A: The post below from a partner fusion center advocates for nationwide armed protests at the state capitols on January 17. The post calls for a peaceful rally and doesn't seem to have gained any traction thus far, but the fusion center wanted participants on the call to know in case there is an armed group that shows up at their state house/capitol on the 17th, for public safety planning and the protection of civil rights and civil liberties.

https://www.reddit.com/r/DEGuns/comments/kpgr1p/peaceful_armed_protest_every_capitol_january_17th/?utm_source=share&utm_medium=ios_app&utm_name=iossmf

A: A number of fusion centers also reported planned car caravans this week and MAGA Drag the Interstate rallies that are reported in conjunction with "Occupy the Capital".

Q: Do any of the suspected threat groups have any known cyber centric TTPs used in the past we are concerned with?

A: There were no reported cyber centric TTPs mentioned on the call.

Q: How will the FBI be tracking threats in eGuardian?

A: FBI eGuardian will be using the tag #CERTUNREST2021 to track, organize and coordinate incoming threats related to the upcoming January 6th, 2021 meeting by Congress to certify the results of the 2020 Presidential Election. Reporting indicates a significant number of individual plan to or are advocating for others to travel to Washington, DC to engage in civil unrest and violence.

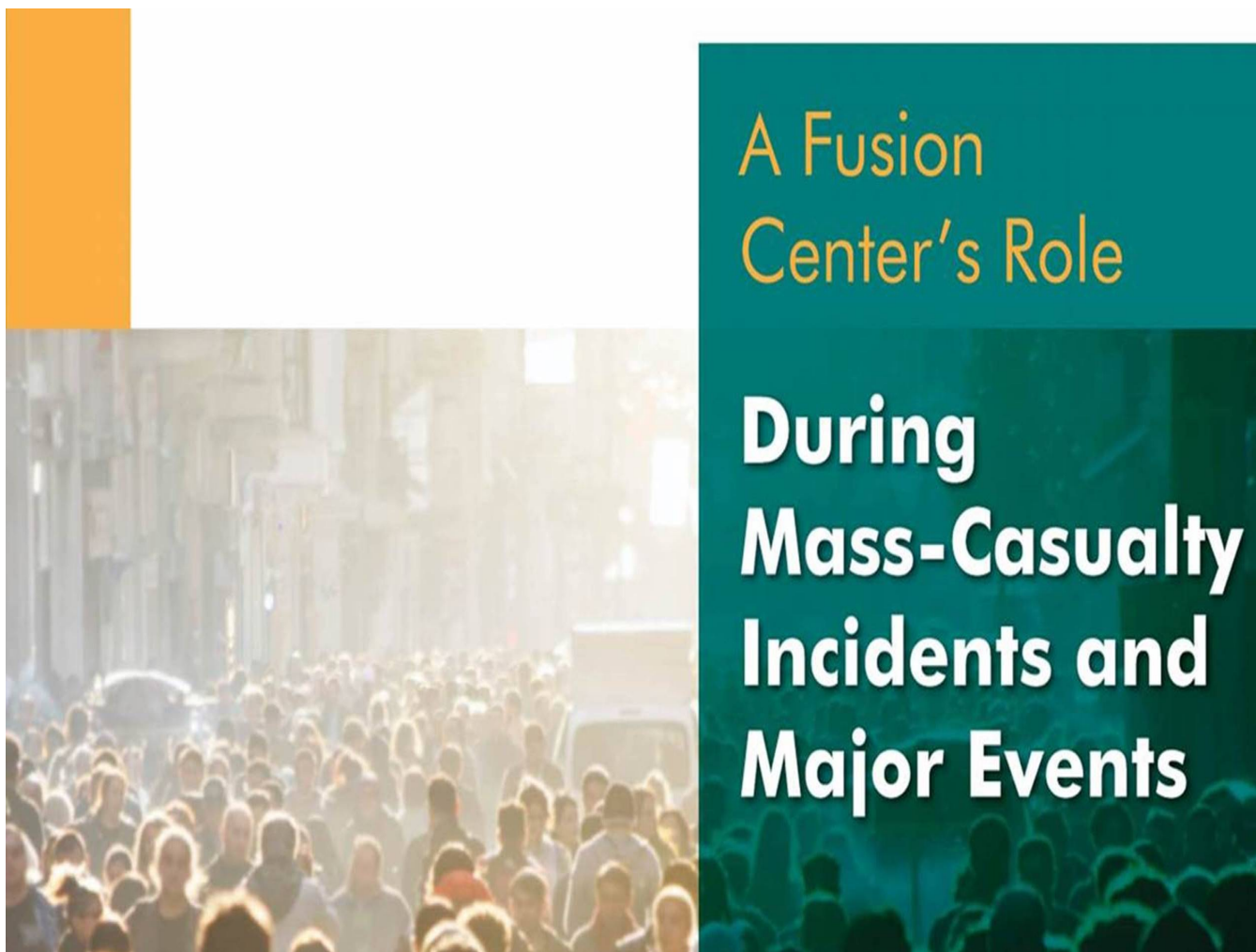
NFCA Privacy Committee Recommended Reading:

<https://it.ojp.gov/documents/d/Recommendations%20for%20First%20Amendment-Protected%20Events%20for%20state%20and%20local%20law%20Enforcement.pdf>

<https://it.ojp.gov/GIST/1200/Real-Time-and-Open-Source-Analysis--ROSA--Resource-Guide>

Recommendations for a fusion center's role during mass-casualty incidents and major events:

I also want to remind partners that if a major physical or cyber threat incident does occur, such as a mass casualty event or major cyber-attack that has a specific point of impact, that the fusion center(s) in the primary impacted area(s) should not be contacted via e-mail, phone, or text. We have the HSIN rooms for communication during these types of incidents and HISN-Exchange for RFI requests that should only be outbound from the impacted center(s). The NFCA will have a single POC that will coordinate with the impacted director(s) to liaison for any support needs. We will also coordinate with the impacted director(s) to host a national conference call as soon as possible to brief the Network. The call will be sent to your e-mail with a calendar invite. We have a capacity for 350 partners on the VTC. For further information on your potential role during a mass casualty incidents and major events, please click on the image or link below.





<https://it.ojp.gov/AT/Documents/A%20Fusion%20Center's%20Role%20During%20Mass%20Casualty%20Events.pdf>

****National Cyber Situational Awareness Room***

The Cyber Intelligence Network (CIN) and the 80 fusion centers that comprise the National Network of Fusion Centers only collect and store information related to suspicious activity reports, tips and leads based on observed behavior reasonably indicative of pre-operational planning associated with terrorism or other criminal activity or where a criminal nexus has been established or determined. The First Amendment protects all forms of speech, including protest and counter-protest activity, except in specific circumstances. Unlawful activity (i.e., threats of violence, acts of violence and cyber-criminal activity) is not protected activity. CIN Members/Fusion Center Leadership and Partners.

CIN Member/Fusion Center Leadership and Partners,

At the request of the National Network of Fusion Centers, and Department of Homeland Security-assigned fusion center personnel, and with staffing support from the Department of Homeland Security (DHS) Cybersecurity and Infrastructure

Security Agency (CISA), the National Cyber Situational Awareness HSIN room will be open to provide cyber threat identification capabilities pertaining to the General Election. The National Cyber Situational Awareness room will be monitoring information sources for any potential threats or situations that could result in violence, a threat to public safety, or a threat to network-connected infrastructure. The participants in the National Cyber Situational Awareness room will also be participating in information sharing with vetted public safety partners and querying for reports of violent protests, civil disobedience, and criminal or terrorist activity regarding the General Elections.

The National Cyber Situational Awareness room will continue operating 24/7 during the general election. During this activation period, the National Cyber Situational Awareness room will be utilized for the sharing of raw cyber intelligence to assist in the identification, triage, assessment, and sharing of potential cyber threats. Cyber Intelligence Network (CIN) members, Cyber Investigators, Cyber Analysts, and Fusion Center Analysts who are permitted to access U//LES information (who are non-CIN members) are also invited to enter the room for this incident. National Cyber Situational Awareness room activations provide an avenue for communications between disparate cyber entities that may not have been connected otherwise. Cyber analysts and investigators across the United States will be empowered to scrutinize and examine open source, FOUO, and LES information to make conclusions and recommendations relative to the current cyber threat landscape, and help organizations implement protective measures. Vetted threat information will be communicated to the appropriate handling agency and the HSIN SitRoom. Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) personnel and National Cyber Situational Awareness room personnel are in constant contact and providing unified situational awareness between the various HSIN room stakeholders.

Entering the National Cyber Situational Awareness Room

National Cyber Situational Awareness Room: <https://share.dhs.gov/cyber>

CIN Members

All CIN members must enter the room with their HSIN account credentials and will automatically be entered into the room.

Guests

Designated non-CIN fusion center and FSLTT personnel and partners can enter the room if required by their organization. Prior to entry, an email must be sent to CINaccess@nfcausa.org by a CIN member or affiliated organization requesting access for that individual(s) to be permitted entry. Please include the individual(s) full name, title, affiliation, and supervisor contact information. Guests will not be allowed access without a prior written request and must enter with their HSIN credentials to enter the room. Access as a "Guest" will be assessed on a case-by-case basis if the non-CIN member does not have a HSIN account. Please feel free to forward this announcement onto those who have a valid need to know and are

permitted access to U//LES information. Guest access for this activation does not constitute CIN Membership and does not inherently grant access for future activations.

About the Cyber Intelligence Network (CIN)

The CIN is an association of cyber analysts and cyber investigators across the country dedicated to responding to cyber incidents, sharing cyber intelligence, and producing relevant, actionable, and timely analytic products on cyber threats. CIN's mission is to support the free and rapid exchange of cyber intelligence. Through the CIN, cyber analysts:

- Share information rapidly,
- Coordinate and prevent the duplication of efforts, and
- Connect with each other, so analysts know who their counterparts are nationwide and can rely on them when needed

The Requirements for Membership are as follows:

- (1) You must have "Cyber Analysis" or "Cyber Investigation" as a designated part of your job. This would include those working in cyber security, threat intelligence, and information warfare.
- (2) You must be cleared to handle Unclassified/Law Enforcement Sensitive (U//LES) information. This includes all law enforcement, fusion center Intelligence Analysts, and any Cyber Analyst with a security clearance Secret or higher.

These requirements are non-negotiable. All members are expected to participate in the Cyber Intelligence Network and be available to assist on national cyber incident response and analytical projects when needed. Additionally, law enforcement sensitive information is shared on the CIN, and we therefore must ensure all members are cleared to handle U//LES documents.

Thank you for your service to the Network and the Nation!

Donell Harvin, DrPH, MPH, MPA
Chief, Homeland Security and Intelligence Executive Director, National Capital Region
Threat Intelligence Consortium (NTIC) District of Columbia Homeland Security and
Emergency Management Agency
2720 Martin Luther King Jr. Ave, SE
Washington, DC 20032
Mobile: 202-531-0451
Email: Donell.harvin@dc.gov
Website: hsema.dc.gov

Mike Sena
President - NFCA
Executive Director

Northern California High Intensity Drug Trafficking Area
Northern California Regional Intelligence Center
P.O. Box 36102 | San Francisco | CA | 94102
415.725.1000
(24 Hr.) 866.367.8847
mseana@ncric.ca.gov

A Fusion Center's Role

During Mass-Casualty Incidents and Major Events





A Fusion
Center's Role

**During
Mass-Casualty
Incidents and
Major Events**



A Fusion Center's Role During Mass-Casualty Incidents and Major Events

Overview

The purpose of this document is to describe a plan for effective response—as well as coordination and communication—during mass-casualty and fatality incidents, major events, and other major critical incidents that leverages fusion center resources¹ and expertise. Critical incidents are resource-intensive and require more comprehensive planning and direction than routine public safety incidents.² This document provides recommendations for fusion centers that do not have existing relationships, protocols, policies, or memoranda of agreement with their federal, state, local, tribal, or territorial (FSLTT) emergency operations centers (EOCs) and law enforcement operation centers. It defines the role and responsibilities of such fusion centers during major critical incidents. A fusion center may play a crucial role by supporting investigations, enhancing the intelligence cycle, and providing situational awareness to FSLTT public safety agencies, as well as private sector and critical infrastructure and key resources (CIKR) partners. The document complements and builds on the *NIMS Intelligence/Investigations Function Guidance and Field Operations Guide*³ as well as the *Considerations for Fusion Center and Emergency Operations Center Coordination Comprehensive Preparedness Guide (CPG) 502*.⁴

Fusion centers may modify their usual operations in response to resource-intensive events in order to provide field intelligence support, consequence management recommendations (when staffed by personnel with the appropriate expertise), and situational awareness information sharing to the affected region, within the state, and to the nation. Consequence management recommendations may be made by emergency management, technical response, and fusion center personnel who contribute intelligence and information to support decision-making efforts. The fusion center also may provide support to the incident command structure through the request for information (RFI) process. After key stakeholders and law enforcement agencies in the area of responsibility (AoR) have addressed public safety concerns following an event, fusion centers may provide on-scene liaison and/or case support to law enforcement agencies, sharing approved information between homeland security partners and the incident command. The fusion center should support the incident command structure (ICS) through direct liaison involvement during a response by the primary emergency management

¹ Fusion center resources are available from a number of locations, including the U.S. Department of Homeland Security ([DHS](#)), the Office of the Director of National Intelligence ([ODNI](#)), the National Fusion Center Association ([NFCA](#)), the National Criminal Intelligence Resource Center ([NCIRC](#)), and Global Justice Information Sharing Initiative (Global) [Toolkit](#) sites.

² Critical incidents include both human-made and natural disasters. While this document focuses on human-made disasters, there is also application for preparing for and responding to natural disasters.

³ Available at: <https://www.fema.gov/media-library/assets/documents/84807>.

⁴ Available at: <https://www.fema.gov/media-library/assets/documents/25970>.

organization and not through a structured RFI process.⁵ “Flat” information sharing is critical when mitigating an incident. Fusion centers are capable of enhancing information sharing, both regionally and nationally, because of their ability to utilize support from partners—including the National Network of Fusion Centers (NNFC) and partner fusion liaison officers (FLOs), Federal Bureau of Investigation (FBI) field intelligence groups (FIGs) and FBI Joint Terrorism Task Force (JTTF) members, Regional Information Sharing Systems® (RISS) Centers, High Intensity Drug Trafficking Area Investigative/Intelligence Support Centers (HIDTA ISCs), FEMA regional offices,⁶ and private sector/critical infrastructure partners—to gather incident-related information. They can support an emergency operations center (EOC) and/or law enforcement operation center’s incident management activities, including incident or natural disaster responses and short-term recovery efforts.

Designated and qualified fusion center personnel, as identified in an agreement/memorandum of understanding (MOU), standard operating procedures (SOP), concept of operations (CONOP), or business plan, also may be tasked with reporting to an incident scene or supporting the incident from the EOC and/or law enforcement operation center. Fusion center personnel and EOC and law enforcement operation center personnel should regularly engage in joint support operations during large planned events to provide improved collaboration during major and unplanned events, such as mass-casualty incidents.⁷

A key task for fusion center personnel serving in a collection and reporting capacity is to support the coordinated dissemination of accurate and approved near-real-time information from the fusion center responsible for directly supporting the event or incident. The capacity to share information may be supported and/or enhanced by nearby major urban area fusion centers, nearby state fusion centers, and the National Network of Fusion Centers or fusion center partners in the field. Alerts, including National Terrorism Advisory System (NTAS) alerts, must be transmitted as accurately and timely as possible to law enforcement, public safety, and homeland security agencies and departments in the affected region, within the state, and to the nation. Promptly transmitting and/or relaying alerts will ensure that all partners are aware of incidents as they develop and reduce the proliferation of inaccurate information. Information sharing platforms, such as the [Homeland Security Information Network-Intelligence’s \(HSIN-Intel\) Situational Awareness Room \(SitRoom\)](#), Web-based email/text alert platforms, and/or video/voice teleconference calls, should be included in a fusion center’s dissemination plan.

This document outlines some of the fusion center’s roles, activities, and necessary capabilities throughout the incident process, including pre-incident planning, potential forward deployment of personnel in concurrence with the lead investigative agencies, data collection, analysis, communications, support to the EOC or law enforcement operation center, and transition to recovery.

⁵ See *NIMS Intelligence/Investigations Function Guidance and Field Operations Guide*.

⁶ A list of FEMA regional offices is available at <https://www.fema.gov/fema-regional-office-contact-information>.

⁷ MOUs, agreements, and plans that outline cooperation and commitments should be established prior to an incident, and the lack of an MOU or agreement should not deter information sharing while attempting to mitigate a critical incident.

Pre-Incident Planning Stage

In the pre-incident planning stage, fusion centers should ensure that appropriate MOUs, agreements, plans, training, readiness to leverage associated information sharing systems, and establishment of a request for assistance and notification process have been developed and implemented.⁸

Training

Pre-incident planning should include training on the following capabilities, activities, and resources:⁹

- Information sharing systems access
- Tactical analytical production and dissemination
- Real-Time and Open Source Analysis (ROSA)¹⁰
- National Incident Management System (NIMS)—The following Federal Emergency Management Agency (FEMA) Independent Study Program training courses should be completed by all fusion center personnel supporting critical incidents, major investigations, and special events:¹¹
 - [IS – 100](#): Intro to Incident Command System
 - [IS – 200](#): Basic Incident Command System for Initial Response
 - [IS – 700](#): An Introduction to the National Incident Management System
 - [IS – 800](#): National Response Framework, An Introduction

In addition to pre-incident training, fusion centers and jurisdictional partners should coordinate and conduct joint scenario-based tabletop and live training exercises to assess plans, SOPs and MOUs. Fusion center leadership should also work with FSLTT emergency management offices to assist in the identification of additional relevant training related to critical incident response and the role of on-scene personnel.

⁸ The *Considerations for Fusion Center and Emergency Operations Center Coordination Comprehensive Preparedness Guide (CPG) 502* provides additional guidance related to fusion center and EOC coordination, with a focus on pre-incident planning.

⁹ This resource focuses on the role of the fusion centers; however, fusion center partners also should consider applicable training on relevant systems and processes.

¹⁰ For more information, see *Real-Time and Open Source Analysis (ROSA) Resource Guide: Understanding and Using Open Source Resources for Law Enforcement Operations* [resource under development].

¹¹ The full catalog of FEMA online training offerings is available at <https://training.fema.gov/is/crslst.aspx>. Moreover, *Considerations for Fusion Center and Emergency Operations Center Coordination Comprehensive Preparedness Guide (CPG) 502* identifies additional training resources applicable to fusion center personnel.

Information Sharing Systems

Fusion center preparation for a critical incident response should include coordination with FSLTT partners (including EOC and law enforcement). Fusion centers should provide outreach and training regarding the role of the fusion center and pre-incident access to appropriate information sharing systems, including the fusion center's information distribution mechanism(s), Homeland Security Information Network (HSIN), the Law Enforcement Enterprise Portal (LEEP), and one of the three interconnected [nationwide event deconfliction systems](#):¹² the RISS Officer Safety Event Deconfliction System (RISSafe™), the Secure Automated Fast Event Tracking Network (SAFETNet), or the Washington/Baltimore HIDTA's Case Explorer. All of these systems typically require registration of individual officers and staff members *prior to a critical incident* to gain access to the full functionality of these applications. All appropriate information sharing agreements and access should be addressed prior to an incident to reduce information sharing issues during an incident.

- **HSIN-Intel, HSIN SitRoom and HSIN Exchange**

HSIN-Intel¹³ facilitates the sharing, dissemination, and notification of key Sensitive But Unclassified (SBU) intelligence information among federal, state, local, tribal, and territorial (FSLTT) stakeholders. HSIN-Intel was established to support the critical intelligence information sharing needs of the Homeland Security Information Sharing Environment. HSIN-Intel provides value to critical stakeholders by fusing comprehensive security and collaboration technologies with appropriate governance.

The HSIN-Intel collaboration environment supports the unique requirements of more than 10,000 users. It utilizes two-factor authentication for the protection of approved personally identifiable information within specific collaboration areas and leverages solid vetting and user management, optimized to support both automated and manual business processes. HSIN-Intel collaboration tools are tailored to the needs of the stakeholder community; the portal-based collaboration platform provides access via an extranet connection. Each tool incorporates rigorous security disciplines, such as compartmentalization, need-to-know management, and granular logging and audit features.

HSIN SitRoom is a centralized, 24/7 Adobe Connect virtual information sharing room that provides all trained HSIN-Intel members with a means to monitor and post relevant items related to an ongoing incident of national or regional significance. The Adobe Connect platform allows users to communicate and share documents, presentations, and video.

¹² Additional information on event deconfliction is available at <https://www.ncirc.gov/deconfliction/> and in *A Call to Action: Enhancing Officer Safety Through the Use of Event Deconfliction Systems* at <https://it.ojp.gov/gist/149/File/event%20deconfliction%20call%20to%20action0.pdf>.

¹³ For more on HSIN-Intel, visit <http://www.dhs.gov/sites/default/files/publications/HSIN-Fact%20Sheet-HSIN-Intel.pdf>.

HSIN Exchange provides the national network of fusion centers, High Intensity Drug Trafficking Areas (HIDTAs), the Terrorist Screening Center (TSC), and the El Paso Intelligence Center (EPIC) with a secure, standardized way to submit, respond to, and easily track RFIs.¹⁴ As a centralized RFI management system, HSIN Exchange reduces the duplication of systems and effort while making it easy for analysts to pick up and continue work from one shift to the next.

- **FBI's Law Enforcement Enterprise Portal (LEEP) Virtual Command Center**

The FBI's Law Enforcement Enterprise Portal (LEEP) is a centralized location for law enforcement agencies, intelligence groups, and criminal justice entities to access beneficial resources. These resources may help investigators strengthen case development and enhance information sharing between agencies.

LEEP services, resources, and systems access include the following:

- [National Data Exchange \(N-DEx\)](#)
- [Intelink](#)
- [Regional Information Sharing Systems Network](#) (RISSNET™)
- [National Gang Intelligence Center](#)
- [Internet Crime Complaint Center \(IC3\)](#)
- Virtual Command Center (VCC) is a situational awareness and/or crisis management tool used to share information about street-level and tactical activities among law enforcement operations centers.

- **Requests for Assistance and Notifications**

Any member of a fusion center who becomes aware of a mass-casualty incident or planned major special event that may attract terrorist or other criminal threats must notify the fusion center management as soon as possible and follow agency and ICS procedures. This includes:

- Notifying the appropriate FSLTT law enforcement, homeland security, public health, or emergency management agencies that have the primary responsibility for threat identification, prevention, mitigation, response, recovery, and/or investigation for the incident or event.
- A designated management team member or his or her designee should coordinate information sharing, within the scope of the fusion center's privacy policy, with the primary law enforcement jurisdiction, the FBI, and the emergency management resources where the event is located, as well as with ATF with respect to national response capabilities within the National Response Framework ESF-13.¹⁵ If ESF-13 is not activated, fusion center

¹⁴ It is anticipated that HIDTA ISCs, RISS Watch Centers, and other field-based intelligence entities will have access to HSIN Exchange.

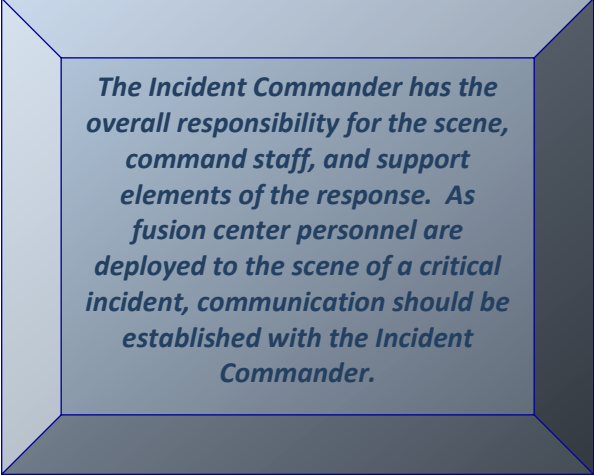
¹⁵ ATF is the executive agency responsible for Emergency Support Function (ESF) 13 as part of the National Response Framework.

personnel should consider supporting the planning section at the command post, law enforcement operations center, and/or EOC (or other on-site command center).

- If adequately trained personnel are available within the fusion center, the fusion center may offer assistance and, conversely, notify the fusion center management team of any requests for support.
- In the case of a potential act of terrorism or mass-casualty incident, the designated fusion center management team member or his or her designee should ensure that notifications are also made through any existing process to HSIN Connect—SitRoom, the FBI JTTF/FIG, the U.S. Department of Homeland Security (DHS) Office of Intelligence and Analysis (DHS I&A), the DHS National Operations Center (NOC), the primary state fusion center/major urban area fusion center, the state homeland security advisor (HSA), or the National Network of Fusion Centers (NNFC).

Forward Deployment of Fusion Center Personnel

To maximize the use of resources, enhance the quality of information being produced, and improve the efficiency of information sharing (during critical incidents, the first point of failure is often communication), fusion center personnel may potentially be forward-deployed in concurrence with the incident commander and lead investigative agencies as necessary to support resource-intensive critical incidents or events. Fusion center personnel also may be deployed to the EOC and/or law enforcement operation center to support ESF-13, assisting the EOC with analytical capabilities and serving as a conduit to communicate with and exchange information with forward-deployed fusion center personnel, the intelligence community, and our nation's fusion center partners through the National Network of Fusion Centers.



The Incident Commander has the overall responsibility for the scene, command staff, and support elements of the response. As fusion center personnel are deployed to the scene of a critical incident, communication should be established with the Incident Commander.

Designated and qualified fusion center first responders may potentially be forward-deployed near the location of a critical incident for the primary purpose of coordinating situational intelligence and information sharing support after immediate life-threatening public safety concerns are addressed. Unless otherwise designated by the lead investigative agency, forward-deployed fusion center personnel are on-scene as an intelligence and information sharing support entity and not as an enforcement and investigative entity. The role of an on-scene, forward-deployed fusion center first responder may be to assist the incident commander/lead investigative agency with the establishment of the Joint Intelligence Operations Center (JIOC), if established as a part of the ICS, and the connection to the fusion center's information and intelligence resources. Qualified fusion center personnel may act as or support the intelligence operations section chief for the incident, as described in the [NIMS Intelligence/Investigations Function Guidance and Field Operations Guide](#). Deployed fusion center

personnel should have multiple communications platforms that support data connectivity for voice, video, and text through satellite and cellular systems.

Fusion center personnel deployed to the EOC and/or law enforcement operation center can serve as channels to communicate with and exchange information with the FSLTT intelligence resources. Fusion center representatives also serve to support personnel on-site at an incident, providing analytical support and enhancing capabilities to other resources.

Joint Intelligence Operations Center

If a JIOC has been established, immediately upon arrival near the scene, the fusion center manager or designee should work with the incident commander or Joint Intelligence Operations Center (JIOC) commander to identify needed information and analytical support and then establish an intelligence and information sharing presence at the scene and a JIOC or desk. The JIOC should be a collaboration among the responding agencies' intelligence analysts, intelligence officers, and the fusion/threat/terrorism liaison officers (FLOs/TLOs). It should coordinate situational awareness and the request for information (RFI) process.

The JIOC should be, if possible, independent of the scene of an incident, and the location should be secured by uniformed or fusion center personnel with the appropriate and authorized safety equipment. According to NIMS guidance, JIOC leadership should consider locating their JIOCs at locations that have the following resources, if possible.

- Utilities, such as electric, telephone service, and internet connectivity
- Agency portable radios
- Satellite telecommunications devices, cellular telephones, Wi-Fi hot spots, computers, and multipurpose printers
- Access to software tools, law enforcement/open source databases, and GIS applications
- Projectors, projector screens, whiteboards, and area maps
- Portable locking file cabinets for extended operations
- Office supplies, such as pens, markers, notepads, staplers

The following is a list of tasks and actions that fusion center first responder personnel may consider when initially establishing a JIOC/intelligence section or desk.

- Coordinate with the lead law enforcement agency to support the agency's role in public safety information sharing, serve as a collection point for information, and support the lead agency's personnel in releasing information, as needed.
- Collect and evaluate information while responding to an incident scene.
- Obtain a comprehensive briefing regarding an incident.
- Confer with the incident or JIOC commander regarding how the JIOC Intelligence and Public Safety Information Sharing Section should be established and organized. If there is no intelligence commander/supervisor on-scene, coordinate with the incident commander regarding the Intelligence and Public Safety Information Sharing Section and ensure that incident personnel are promptly notified.
- Confer with the incident or JIOC commander to determine which intelligence and investigative agencies are involved in the incident. The involvement of some agencies may be required by law.
- Ensure that:
 - Intelligence activities are expeditiously implemented.
 - Life safety operations objectives take priority over all other incident objectives. However, in extraordinary emergency circumstances, intelligence activities may be initiated concurrently with life safety operations.
 - Required audio, data, image, and text communications equipment is obtained and communication procedures are implemented in conjunction with the fusion center's or primary/supporting law enforcement agency's/agencies' information technology team.
 - A specific verbal or, if applicable, written Intelligence Section Communications Plan is prepared and provided to the Logistics Section.
 - An Operations Section technical specialist is assigned to the Intelligence Section work area.
 - An Intelligence Section technical specialist is assigned to the Operations Section work area.
 - Intelligence Section staging areas are activated and a staging area manager is designated for each staging area as needed.
 - Resources that initially responded to the scene and resources that are subsequently requested are immediately identified and checked in and out.

Active Incident Response/On-Scene Fusion Center Roles and Responsibilities

The fusion center(s) engaged in supporting an incident should be responsible for supporting two major functions: information intake/assessment and information/intelligence management. Because the configuration of the Incident Command System (ICS) organization is flexible, the incident or JIOC commander may choose to combine these functions or create teams to perform these functions.

For states with multiple fusion centers or state and major urban area fusion centers that are near each other, it is critical to streamline the coordination of responsibilities of each center at the beginning of the event response to deconflict resource deployment and improve efficiency.

Information Intake and Assessment:

The information intake/assessment function ensures that incoming information that is collected, except the results of investigative leads/tasks, is:

- Communicated directly to the Intelligence Group within the Incident Command System.
- Documented on an information control form and/or entered into the fusion center's Intelligence Management System and/or the FBI's ORION system.
- Evaluated to determine the correct information security designation (e.g., Law Enforcement Sensitive or For Official Use Only) and the required information security procedures.
- Initially evaluated and categorized as being information that:
 - May require the Investigative Operations Group to assign an investigative lead/task (this information is communicated to the Investigative Operations Group for final assignment determination).
 - Constitutes intelligence but does not require the Investigative Operations Group to assign an investigative lead/task (absent unusual circumstances, this information is communicated to the Investigative Operations Group).
- Coordinated with the appropriate federal agency to develop tear-line information from classified information and/or access-controlled sensitive compartmented information and/or caveated/restricted information to sanitize the information for use in tasks and activities, including supporting investigative leads/tasks, publishing intelligence products, and preparing warrant applications and accusatory instruments.
- Appropriately disseminated (i.e., intelligence/investigations information, documents, requirements, and products are appropriately disseminated).
- Immediately transmitted (i.e., vetted accurate threat information/intelligence is immediately transmitted to the incident commander, the Operations Section chief, and, if necessary, other authorized personnel).

Other fusion center activities, roles, and responsibilities associated with the information intake and assessment function may include:

- Notifying and conferring with subject-matter experts.
- Identifying and collecting intelligence/investigations information.
- When applicable, ensuring that requests for intelligence/investigations information are documented, analyzed, managed, and resolved.
- Conferring with the Planning Section regarding information/intelligence-related activities as needed.
- Activating one or more of the following positions, by the on-scene fusion center supervisor or manager:¹⁶
 - Information intake and assessment manager
 - Requirements coordinator
 - Collection coordinator
 - Processing and exploitation coordinator
 - Analysis and production coordinator
 - Dissemination coordinator
 - Critical infrastructure and key resources protection coordinator
 - Classified national security information security officer
 - Information coordinator

Information/Intelligence Management

The information/intelligence management function activities include, but are not limited to, ensuring that:

- Tactical and strategic intelligence/investigations information is collected using appropriate, authorized, and lawful techniques and activities that protect privacy, civil rights, and civil liberties.
- Intelligence requirements are used to manage and direct intelligence collection efforts.
- Database and record queries are performed.
- Language translation, deciphering, and decryption services are provided; fusion center partner organizations may be enlisted to support this function.
- Intelligence/investigations information is documented, secured, organized, evaluated, collated, processed, exploited, and analyzed.

¹⁶ Depending upon the size, complexity, and scope of the Intelligence and Investigations Support Section.

- Intelligence information needs, requests for information/intelligence, intelligence gaps, and standing and ad hoc intelligence requirements are identified, documented, analyzed, validated, produced (if applicable), and resolved.
- Requests for intelligence/investigations information are made to the appropriate governmental agencies, nongovernmental organizations, private sector entities/individuals, the media, and the public.
- Finished and, if appropriate, raw intelligence/investigations information is documented and produced as needed (e.g., records, data, warnings, situation reports, briefings, bulletins, and/or assessments).
- Sensitive But Unclassified (SBU) or lesser classified tear-line reports are produced regarding appropriate classified and unclassified information.

Communications

Deployed fusion center personnel should have multiple communications platforms that support data connectivity for voice, video, and text through satellite and cellular systems.

- **Radio Channels**—the primary agency or jurisdiction should provide portable radios utilizing the appropriate law enforcement frequencies. Radios should be used to monitor events and communicate with incident commanders as needed.

The incident commander should be asked to:

- Notify the JIOC of communication protocols.
 - Designate a channel for information sharing from the JIOC.
 - Notify the JIOC of further communications needs.
- **Other Communication Capabilities and Resources: Hard Lines, Cell Phones, Email, Web Portal, Mobile Device Applications, and Conference Calls**

The fusion center's role should be to establish primary and alternate contact methods, such as phone numbers, emails, Web portals, and/or mobile device applications, which should be monitored at the fusion center or JIOC to field inquiries from the National Network of Fusion Centers (NNFC) and field-based information sharing entities not handled on HSIN Connect—SitRoom or HSIN Exchange.

HSIN Connect—SitRoom, HSIN Exchange, and alternate contact mechanism(s) should be monitored by JIOC staff members to ensure that timely responses to information requests are fulfilled. Detailed requests requiring multiple responses should always be processed through HSIN Exchange when possible.

The FBI Office of Partner Engagement (FBI-OPE), DHS Office of Intelligence & Analysis (I&A), and the National Fusion Center Association ([NFCA](#))¹⁷ should coordinate an initial conference call with nationwide homeland security partners and field-based information sharing entities as soon as practical after a major criminal mass-casualty incident. The fusion center's role is to ensure that the local FBI field office, state homeland security advisor, and any supporting field-based intelligence leaders and entities are invited to participate in the call, the purposes of which include providing a regional and national situational report (SitRep) and determining a timeline for the next conference call.

Data Collection Stage

After lifesaving and security measures are performed, the first stage of a fusion center's response to a critical incident is the data collection stage, in which a careful and deliberate process of information collection is formulated and carried out. The working groups for this stage are broken down into a Data Collection Team and a Tips and Leads Team.

- **Data Collection Team**

The Data Collection Team should be responsible for determining the priority intelligence needs and requirements of incident commanders and investigators. Personnel assigned to this team should gather information in the field and through any lawfully available sources. Forward deployment of fusion center intelligence officers and analysts to critical incidents should facilitate the flow of accurate and timely information to the fusion center and its partners.

The Data Collection Team should consist of command-level personnel, senior officers, and intelligence staff members from the following:

- The Incident Command (IC) group
- The fusion center's management, intelligence officers, and analysts
- The primary FSLTT law enforcement agencies
- The National Network of Fusion Centers (NNFC)
- Other FSLTT agencies and/or outside resources as appropriate

This team is responsible for receiving classified and unclassified homeland security, intelligence, counterterrorism, and other criminal threat information from FSLTT public safety partners and private sector entities within its jurisdiction.

Steps involved in supporting the continued receipt of information from identified partners include the following:

¹⁷ To learn more about the benefits of membership in the National Fusion Center Association (NFCA), visit www.nfcausa.org.

1. Establish priority information needs (PINs) for the incident.
2. Determine sources for fulfilling PINs.
3. Develop RFIs in coordination with the lead investigating agency to support incident management. Typical RFI data includes:
 - Suspect and persons of interest
 - Vehicles
 - Locations
 - Weapons data
 - Phone data
 - Assets
 - Businesses
 - Critical infrastructure/key resources (CIKR) threats
 - Similar suspicious incidents
 - Property
4. Designate the primary databases to gather case data and criminal intelligence.
5. Designate the primary shared platforms and common portals on both the classified and unclassified levels. Post RFIs to the designated primary network(s) and systems, which may include:
 - HSIN
 - LEEP
 - Other law enforcement networks as required
6. Develop additional information collection procedures as needed using open source, social media, and public safety data systems.

- **Tips and Leads Team**

The Tips and Leads Team is responsible for establishing a business process to receive and triage tips and leads received from public safety personnel, CIKR partners, witnesses, and the general public through existing Web portals and telephone tip lines. The Tips and Leads Team should identify information and investigative support requirements in conjunction with the primary investigative agency. Tips and Leads Team members may be located either in proximity to the incident scene, at a nearby communications or public safety answering point (PSAP), and/or at the fusion center's offices.

The Tips and Leads Team should consist of call takers or dispatchers from:

- The fusion center.
- The local police public safety agency or PSAP.
- Other federal, state, local, and tribal public safety agency or outside resources as appropriate.

The JIOC manager or designee should have overall authority over the Tips and Leads Team, including ensuring that the following processes and tasks are implemented:

- Intake of tips and leads should include using a standard entry format, such as a field interview or a suspicious activity reporting form.
- Tips and leads are reviewed for data quality and the need for further clarification.
- Tips and leads are entered into a database or similar application for storage and routing to investigators.
- The fusion center manager or designee should ensure that tips and leads inform decision making by the analytical production teams.

Data Analysis Stage

- **Analytical Production Stage**

This stage should divide work between the Investigative Support Team and the Situational Awareness Production Team. These teams should provide analytical products to support the investigation as well as provide situational awareness reports to responding agencies and partner agencies. Whenever possible, both of these teams should consist of analysts from the fusion center, the local law enforcement agency, the FBI Field Intelligence Group (FIG), DHS Office of Intelligence & Analysis intelligence and/or reports officers, and other state and federal agencies, as appropriate.

- **Investigative Support Team**

The Investigative Support Team should reinforce investigative priorities through fact checking, database searches, and social media analysis, as needed. **Important note: Because social media is such a timely and ubiquitous communication mechanism, appropriate monitoring is critical to ensure continued access for investigative purposes.** As such, all fusion center personnel—whether responding to a critical incident or working in a steady state—are urged to review [*Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities: Guidance and Recommendations*](#).¹⁸

Common analytic services provided by the Investigative Support Team include the following:

- Suspect profile and background checks
- Link analysis and social networking analysis
- Business record analysis
- Telephone toll, pen register, and record analysis
- Financial analysis

¹⁸ This document is available at <https://it.ojp.gov/GIST/132>. To explore additional social media- and privacy-related resources and guidelines, visit <https://it.ojp.gov/GIST/Search?term=social+media>.

- Social media analysis
- Geospatial analysis

Steps in Investigative Support Team activities are as follows:

1. Receive requests for investigative support, such as database queries or social media analysis.
2. Assign task to analyst.

Complete investigative checklist of database searches and deconfliction.

- Law enforcement database checks should include searches of the suspect's criminal/law enforcement contact history, associated address(es), vehicle(s), firearm(s), social media account(s), and phone number(s) through:
 - National Data Exchange (N-DEx)
 - EPIC Portal
 - Organized Crime Drug Enforcement Task Force (OCDETF) Fusion Center Portal
 - FBI's SENTINEL System
 - Statewide/regional criminal justice data, records management system (RMS), and computer-aided dispatch (CAD) data, as well as other government licensing and services data repository systems
- Deconfliction of undercover operations, surveillance, and executing search warrants, as well as targets of investigation and their associated data points, must be performed through one of the [nationwide event deconfliction systems](#), in coordination with the primary investigating agency.

3. Submit completed tasking to supervisor for review.
4. Supervisor or analyst returns completed tasking to investigator-requestor.
5. Supervisor follows up to ensure that no further actions are required and to obtain feedback on the products completed to improve the production cycle.

- **Situational Awareness Production Team**

Steps in Situational Awareness Production Team activities and document production are as follows:

1. Receive request for intelligence or SitRep.
2. Conduct intelligence production meeting.

3. Receive reporting information from fusion center intelligence officers and/or analysts in the field.
4. Draft intelligence or SitRep.
5. Determine document classification. Document(s) should be produced at the lowest classification level for distribution to the widest stakeholder base available to the fusion center.
6. Carry out peer review of draft product.
7. Complete supervisory review of draft product.
8. Obtain fusion center management approval (if required).
9. Disseminate information/intelligence product.
10. Evaluate product using feedback from end users.
11. Continue to identify, maintain, and update fusion center and partner needs and information/intelligence requirements.

- **Real-Time and Open Source Analysis (ROSA)**

Critical incidents may require utilization of real-time and open source information for analysis and situational awareness/assessment reports, intelligence development, and criminal investigations. To support authorized SLTT and federal law enforcement and public safety agencies, the fusion center utilizes ROSA tools to gather and analyze publicly available information on open source platforms for a legitimate law enforcement purpose within the scope of the fusion center's privacy policy. One type of open source information—publicly available information derived from social media—can be a valuable source of information for law enforcement in its crime-prevention and response role. Social media platforms allow users to create, share, and/or exchange user-generated content and ideas in virtual communities and networks.

It is imperative to note that ROSA must be accomplished in balance with the protection of public safety and the protection of the privacy, civil rights, and civil liberties of citizens. As such, a fusion center should have a ROSA policy to establish guidelines for the use of ROSA when appropriate. This policy should define a minimum set of guidelines that govern the use of ROSA and should be established to protect individuals' privacy, civil rights, and civil liberties, ensuring that ROSA and related tools are used appropriately.

While on duty, fusion center personnel may utilize ROSA and related tools only for valid law enforcement/public safety purposes, including:

- Identification of threats to public safety.
- Identification of threats to the community.
- Identification of threats to law enforcement and other first responders.
- Gauging public perception.
- Crime analysis.
- Development of criminal intelligence for situational assessment/awareness.
- Support of criminal investigations.

Fusion center personnel should utilize ROSA only to seek or retain information that is:

- Based on a criminal predicate or threat to public safety; or,
- Based on reasonable suspicion that an identifiable individual (regardless of citizenship or U.S. residency status) or organization has committed an identifiable criminal offense or is involved in or is planning criminal conduct or activity that presents a threat to an individual, the community, or the nation and that the information is relevant to the criminal conduct.

Fusion center personnel should not utilize ROSA to seek or retain information about:

- Individuals or organizations solely on the basis of their religious, political, and/or social views or activities;
- An individual's participation in a particular noncriminal organization or lawful event;
- An individual's race, ethnicity, citizenship, place of origin, disability, gender, or sexual orientation unless such information is relevant to the individual's criminal conduct or activity or is required to identify the individual; or
- An individual's age other than to determine whether someone is a minor.

Fusion center personnel should not directly or indirectly receive, seek, accept, or retain information from:

- An individual or nongovernmental information provider who may or may not receive a fee or benefit for providing the information if there is reason to believe that the information provider is legally prohibited from obtaining or disclosing the information; or
- A source that used means to gather the information that may be prohibited by either law or policy.

Transition to Recovery Stage

The incident commander should determine the transition from the active incident response stage to the recovery stage. At this point, a decision should be made to transition the intelligence and information sharing function to a steady state.

Activities and roles in which fusion center personnel should be involved include designating the last SitRep, determining to continue or transition the tip line, debriefing information sharing/investigative teams, and constructing an after-action report.

Additional Resources

To assist fusion centers and other partners in planning for incident response efforts, additional resources are available, including:

- *NIMS Intelligence/Investigations Function Guidance and Field Operations Guide*, <https://www.fema.gov/media-library/assets/documents/84807>
- *Considerations for Fusion Center and Emergency Operations Center Coordination Comprehensive Preparedness Guide (CPG) 502*, <https://www.fema.gov/media-library/assets/documents/25970>
- Fusion Centers and Emergency Operations Centers (an overview), <https://www.dhs.gov/fusion-centers-and-emergency-operations-centers>
- *Fusion Center Guidelines*, <https://it.ojp.gov/GIST/94/Fusion-Center-Guidelines--Law-Enforcement-Intelligence--Public-Safety--and-the-Private-Sector>
- *Baseline Capabilities for State and Major Urban Area Fusion Centers*, <https://it.ojp.gov/GIST/39/Baseline-Capabilities-for-State-and-Major-Urban-Area-Fusion-Centers>