Global Justice Information Sharing Initiative

BJA
Bureau of Justice Assistance
U.S. Department of Justice

Cyber Integration for Fusion Centers

An Appendix to the *Baseline Capabilities for State and Major Urban Area Fusion Centers*

May 2015

DHS-001-05722-000125

REL0001269770

Cyber Integration for Fusion Centers

An Appendix to the *Baseline Capabilities for State and Major Urban Area Fusion Centers*

May 2015

About the Global Advisory Committee

The Global Advisory Committee (GAC) serves as a Federal Advisory Committee to the U.S. Attorney General. Through recommendations to the Bureau of Justice Assistance (BJA), the GAC supports standards-based electronic information exchanges that provide justice and public safety communities with timely, accurate, complete, and accessible information, appropriately shared in a secure and trusted environment. GAC recommendations support the mission of the U.S. Department of Justice, initiatives sponsored by BJA, and related activities sponsored by BJA's Global Justice Information Sharing Initiative (Global). BJA engages GAC-member organizations and the constituents they serve through collaborative efforts, such as Global working groups, to help address critical justice information sharing issues for the benefit of practitioners in the field.

This project was supported by Grant No. 2013-D6-BX-K001 awarded by the Bureau of Justice Assistance, Office of Justice Programs, in collaboration with the Global Justice Information Sharing Initiative and the U.S. Department of Homeland Security. The opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the U.S. Department of Justice or the U.S. Department of Homeland Security.

DHS-001-05722-000128

REL0001269770

Table of Contents

Introduction 1

Purpose 1

Cyber Community's Role in Meeting the Baseline Capabilities 2

Recognition of the Value Added by Cyber Engagement With Fusion Centers 4

Fusion Center Cyber Toolkit 5

I. Fusion Process Capabilities 7

A. Fusion Center Operational Determination 7

B. Planning and Requirements Development 7

C. Information Gathering/Collection and Recognition of Indicators and Warnings 10

D. Processing and Collation of Information 11

E. Intelligence Analysis and Production 12

F. Intelligence and Information Dissemination 13

G. Reevaluation 13

II. Management and Administrative Capabilities 15

A. Management and Governance 15

B. Information Privacy Protections 16

C. Security 16

D. Personnel and Training 16

E. Information Technology/Communications Infrastructure, Systems, Equipment, Facility, and Physical Infrastructure 17

F. Funding 18

Appendix A: Acronyms 19

Appendix B: Traffic Light Protocol 21

Appendix C: Cyber Incident Severity Schema 23

DHS-001-05722-000129

REL0001269770

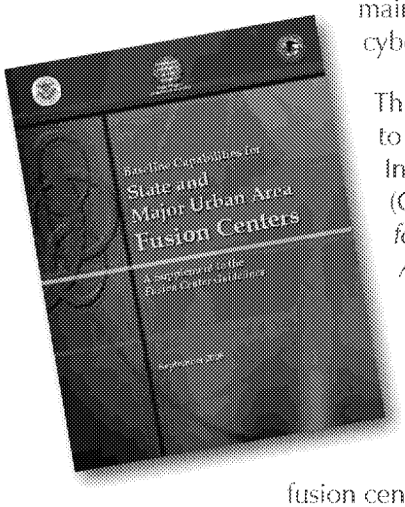
DHS-001-05722-000130

REL0001269770

Introduction

Purpose

This document identifies recommended actions and guidance for state and major urban area fusion centers (fusion centers) to integrate information technology, cybersecurity, and cybercrime[1] prevention (cyber) intelligence and analytic capabilities. Development of these capabilities will inform local, state, and national detection, mitigation, response, recovery, investigation, and criminal prosecution activities that support and maintain the United States' cybersecurity.



This document is an appendix to the Global Justice Information Sharing Initiative's (Global) *Baseline Capabilities for State and Major Urban Area Fusion Centers* (Baseline Capabilities).

This document does not identify additional requirements for fusion centers. Rather, for fusion centers that choose to develop and support a cyber capability, it identifies how the fusion centers can effectively integrate the information, resources, personnel, and expertise of cyber partners,[2] cyber stakeholders,[3] and the cyber community,[4] to enhance fusion center information/intelligence sharing processes. This document also illuminates the value achieved when federal, state, local, tribal, territorial (FSLTT), and private sector organizations work with fusion centers and the many opportunities for establishing relationships with the fusion center.

This document does not identify additional capabilities for fusion centers. Rather, for fusion centers that choose to develop and support a cyber capability, it identifies how the fusion centers can effectively integrate the information, resources, personnel, and expertise of cyber partners, cyber stakeholders, and the cyber community, leveraging these entities' cyber intelligence and expanding fusion center information/intelligence sharing processes.

1 *Cybercrime*, as defined in this document, is "any violation of federal, state, or local statute or malicious or suspicious activity in which a computer, a network, or a device is an integral component of the violation." This definition generally excludes child pornography or identity theft matters.

2 *Cyber partners*, as defined in this document, are "any personnel or entities with whom the fusion center has a Memorandum of Understanding (MOU), a Memorandum of Agreement (MOA), a Nondisclosure Agreement (NDA), or a similar contract."

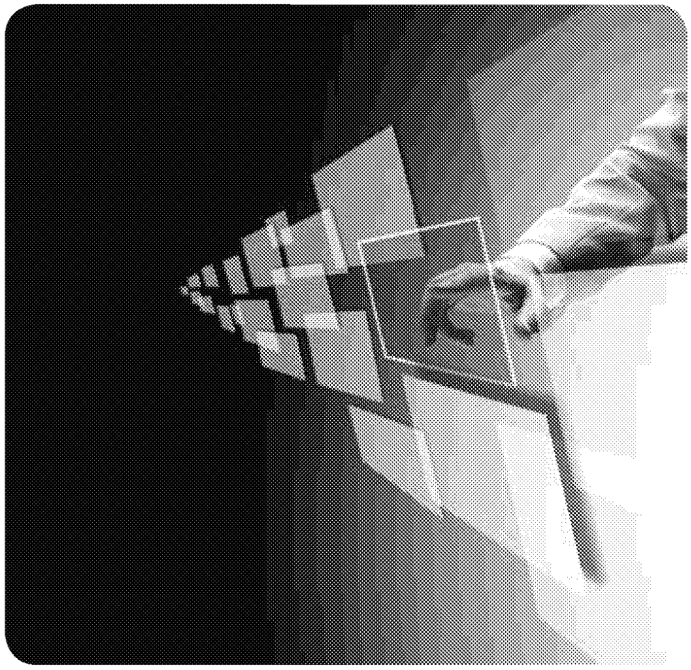
3 *Cyber stakeholders*, as defined in this document, are "any personnel or entities with whom the fusion center has an established, ongoing, and close relationship that involves the exchange of information and/or intelligence."

4 The *cyber community*, as defined in this document, includes "cyber partners, stakeholders, and members of the Fusion Liaison Officer (FLO) program."

DHS-001-05722-000131

REL0001269770

The capabilities in this document are intended to be complementary to those described in the Baseline Capabilities document. They are organized and numbered to correlate directly with the capabilities listed in the Baseline Capabilities document; for example, I.A.1.b or I.A.3.a. For the sake of brevity and clarity, only those items that are directly relevant to the integration of cyber capabilities are included in this document.



Recognizing the value and importance of incorporating cyber capabilities into the fusion process requires an understanding of the evolution of the terms "information" and "intelligence" as they pertain to the current homeland security environment. Though once thought of as relating only to prevention, protection, and investigation missions, information and intelligence are now also recognized as important elements in support of the preparedness for and execution of response and recovery missions. These missions are performed by departments across the emergency services sector, including law enforcement, fire service, and emergency management, as well as cybersecurity and information technology (IT) firms, critical infrastructure (CI) owners and operators, nongovernmental organizations, and the private sector. This document is written on the premise that information and intelligence serve all homeland security partners across all mission areas, and the integration of cyber capabilities can only serve to better prepare all partners.

Cyber Community's Role in Meeting the Baseline Capabilities

The Baseline Capabilities document describes the process, management, and administrative requirements for a fusion center to perform core cyber functions. A fusion center's cyber community may include FSLTT government entities and law enforcement, academia, the private sector, and CI owners and operators. Integrating the cyber community into a fusion center does not require additional core capabilities but simply the incorporation of their information, intelligence, expertise, and resources into the existing fusion center operations.

A cyber attack can be as devastating and effective as a physical attack, while remaining more difficult to detect, mitigate, respond to, recover from, investigate, and prosecute. Incorporating the cyber community will aid a fusion center in achieving its all-crimes and/or all-hazards mission.

---

*The Baseline Capabilities document states that the **all-crimes** approach "incorporates terrorism and other high-risk threats into the existing crime-fighting framework, to ensure that possible precursor crimes are screened and analyzed for linkages to larger-scale terrorist or other crimes." (page 43)*

All-Crimes: Cyberthreats can be integrated into existing crime-fighting frameworks, both as a type of crime and as a component of other terrorism and criminal activity. When provided with training regarding law enforcement's and homeland security's cyber missions and protocols for reporting observed suspicious activities and behaviors, the cyber community can provide fusion centers with information, malicious indicators, and potential precursors of cyber activity, terrorism, and other criminal activity. Such information may include Internet Protocol (IP)

DHS-001-05722-000132

REL0001269770

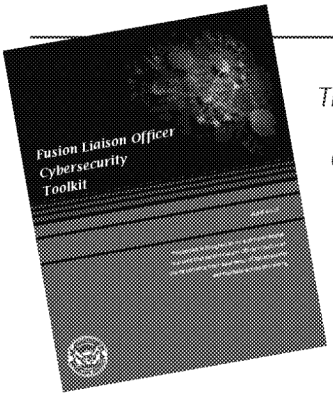
The Baseline Capabilities document states that the ***all-hazards*** *approach "means that the fusion center has identified and prioritized types of major disasters and emergencies, beyond terrorism and crime, that could occur within their jurisdiction and gathers, analyzes, and disseminates information which would assist the relevant responsible agencies...with the prevention, protection, response, or recovery efforts of those incidents." (page 43)*

addresses, signatures,[5] and hashes[6] associated with known malicious activity; detailed information on new tactics, techniques, and procedures (TTPs) or actors; and insight into trends indicative of a pattern of malicious activity. Cyber subject-matter experts (SME) can also provide specialized expertise in interpreting and analyzing raw information, such as log files, malware code, and abnormal computer activity. This may aid fusion centers in achieving a better understanding of threats within a community and nationally. Likewise, fusion centers can share relevant cyberthreat information with the cyber community, such as indicators associated with a new threat actor or a new pattern of activity detected elsewhere and likely to spread into the local area of responsibility (AOR).

All-Hazards: Cyber technology is integral to our way of life, with major disasters affecting cyber infrastructure and capabilities while relying on cyber technologies for recovery. When provided with information regarding the potential effects of natural disasters on cyber infrastructure and capabilities, the cyber community has the potential to aid in prevention, response, and recovery efforts. As incident responders, members of the cyber community are aware of the cyberthreats facing the community; provide detection, mitigation, response, and recovery activities; and are able to assist law enforcement with a variety of surveillance, detection, and prosecution capabilities. The cyber community is embedded in the CI community, which relies on the confidentiality, integrity, and availability of cyber networks. The CI owners and operators can help identify existing vulnerabilities and are also an important part of the response to and recovery from the consequences that various threats present. The perspective of the cyber community adds an important dimension to all-hazards risk assessments, preparedness activities, and mitigation operations.

The relationship the cyber community has with a fusion center depends on a number of factors unique to each AOR. Regardless of capabilities, each fusion center should view the cyber community as important contributors, consumers, and collaborators for its all-crimes and/or all-hazards information and intelligence missions.

- As contributors, cyber community personnel have the ability to share risk information with a fusion center on suspicious activity or cyber indicators and warnings.



The ***Fusion Liaison Officer Cybersecurity Toolkit*** *is designed to be a comprehensive resource that Fusion Liaison Officers (FLOs) can use to enhance their cybersecurity training. The toolkit provides support for FLO training on cybersecurity and cyberthreat indicators and shares best practices on policies and procedures for cyber awareness, reporting, indicators, training, and sharing information in accordance with federal guidance and privacy, civil rights, and civil liberties protections.*

5 Signatures are characteristic or distinctive patterns that can be searched for or that can be used in matching to previously identified attacks.

6 Hashes are a numerical value resulting from applying a mathematical algorithm against a set of data, such as a file. Hashes uniquely identify files, pictures, passwords, etc., such that a comparison of hashed values will determine whether two files, pictures, passwords, etc., are the same.

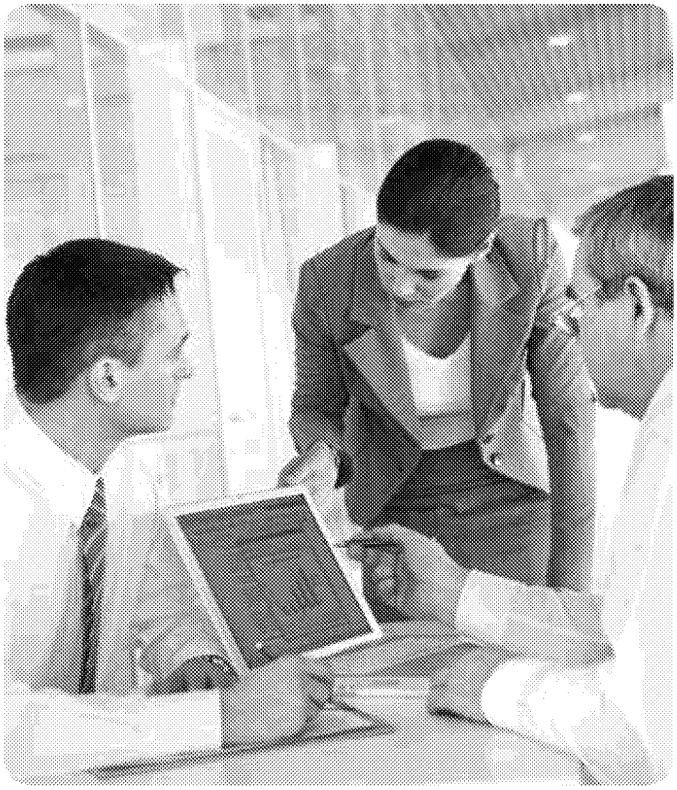
DHS-001-05722-000133

REL0001269770

- As consumers, cyber community personnel have the ability to take action on appropriate and timely unclassified and/or classified threat and situational awareness information and intelligence that will enable them to better guide their preparedness activities and enhance their ability to detect, mitigate, respond to, and recover from the occurrence or indicators of human-caused or natural incidents.

- As collaborators, cyber community personnel have the ability to provide subject-matter expertise and can aid in the receipt, analysis, production, and appropriate dissemination of intelligence products.

Cyber community personnel may be embedded within the fusion center, act as analysts or SME resources for the fusion center, or be members of Fusion Liaison Officer (FLO) programs. Cyber community personnel can also reach back to a multitude of experts and resources within the FSLTT and private sector cyber community, including the personnel and agencies responsible for the cybersecurity of government, private, and CI networks and systems. These extended resources can provide information and intelligence regarding their areas of expertise, including Industrial Control Systems (ICS), cybersecurity and cybercrime, and the development of software, hardware, and emerging technologies, as well as provide contacts within cyber subsectors, including Internet Service Providers (ISP), Web site hosting companies, and mobile platform companies.



Incorporation of the cyber community's information into the fusion center's collection, analysis, and dissemination of information and intelligence processes enhances the collective homeland security effort. Fusion center engagement with the cyber community supports the detection, mitigation, response, recovery, investigative, and criminal prosecution efforts of all homeland security partners through the development, analysis, and sharing of relevant information and intelligence.

Recognition of the Value Added by Cyber Engagement With Fusion Centers

Cybersecurity is one of the most serious economic and national security challenges, and yet it is also one that FSLTT law enforcement, homeland security, and information technology entities continue to struggle to integrate into daily operations. The investigation of computer intrusion matters requires investigators and analysts to possess unique skill sets. However, a wide variety of crimes now incorporate cyber elements, including narcotics, human, and firearm trafficking; counterfeiting; child exploitation; the sale of contraband and illegal goods; fraud; burglary; and homicide, requiring all investigators and analysts to have some level of cyber knowledge.

Fusion centers are uniquely positioned to further cybersecurity objectives by promoting cyberthreat information sharing, analysis, and dissemination between the state, local, and private organizational level and the federal level. The *National Response Framework* (May 2013), the *National Preparedness Guidelines*, the National Institute of Standards and Technology (NIST) Cybersecurity Framework,[7] and multiple Presidential

7 The NIST Cybersecurity Framework is a voluntary framework, based on existing standards, guidelines, and practices, for reducing cyber risks to critical infrastructure, created as a result of Presidential Executive Order 16363—"Improving Critical Infrastructure Cybersecurity." The framework creates a common taxonomy and mechanism for organizations to describe their current cybersecurity posture, describe their target state, identify and prioritize opportunities for improvement, assess progress, and communicate with internal and external stakeholders about cybersecurity risk. Fusion centers can use the framework to learn about the CI owners' and operators' current risk state and determine what information and intelligence may be of value to share.

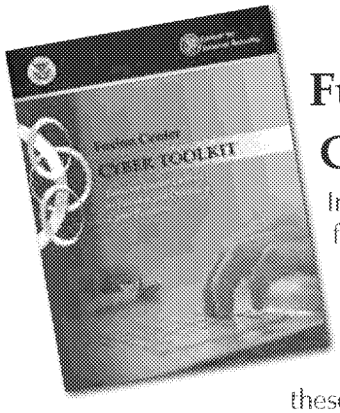
DHS-001-05722-000134

REL0001269770

executive orders have laid out specific capabilities and recommended cybersecurity best practices that include improving the U.S. cybersecurity posture, advocating the migration to more secure technologies, and strengthening information sharing among FSLTT and private sector cyber stakeholders. Supporting programs, such as the U.S. Department of Homeland Security (DHS) Critical Infrastructure Cyber Community C³ Voluntary Program, assist stakeholders in the adoption and use of best practices and relevant information sharing programs.

Improving the national cybersecurity posture requires understanding and sharing information related to malicious cyberactivity, building a network of trusted individuals, aligning operations to create a long-term and sustainable risk management strategy that provides for a changing threat environment, and maximizing the effective use of resources. Fusion centers are focal points for information sharing and are essential in understanding and disseminating information and intelligence. Fusion centers should collaborate with critical cyber partners and/or stakeholders in their region to help ensure that the following resources are in place:

- Access to and participation in a fusion center's robust information sharing processes that allow the movement of relevant and timely open source, unclassified, and classified intelligence and information that support routine and event-specific threat analysis.
- Coordinated cyber policies, programs, and incident response plans that address known and potential threats.
- Exchange of subject-matter expertise.
- Processes that allow for cooperation with law enforcement and prosecutorial efforts.
- The potential for regular and ongoing cyber risk assessments, as well as a process to identify and address sector interdependencies to allow for efficient information sharing and allocation of resources and the response to threats.
- Tools and processes that are flexible and adaptable, allow for rapid adaptation to an evolving threat environment, and incorporate lessons learned and effective practices.



Fusion Center Cyber Toolkit

In recognition of the fact that fusion centers' cyber programs will require certain fundamental components, such as trained cyber personnel, and that individual development of these components may be difficult for a fusion center with limited cyber knowledge, a Fusion Center Cyber Toolkit (Toolkit) for developing a fusion center cyber program is available. Designed as a fusion center cyber program-in-a-box, the Toolkit contains a series of documents that can guide fusion centers in building and running their cyber programs. Included in the Toolkit are:

- Job descriptions for strategic, technical, tactical, and supervisory intelligence analysts and a sworn cyber investigator position.
- A chart identifying the key knowledge, skills, and abilities (KSAs) that cyber personnel should develop within the first year.
- A cyber career path outline with general recommendations for developing cyber personnel's KSAs.
- A list of available organizations, campaigns, training, resources, and assessments that may assist in KSA development or outreach efforts.
- A limited list of industry standard certifications that cyber personnel may reference during the job application process or during their careers.
- A cyber intake questionnaire template that may be used to guide responses to cyber callers.
- Communications maps to guide outreach efforts.
- A cyberthreat actor definition to ensure that fusion centers use definitions similar to those in use by federal and other agencies.
- A copy of the *DHS National Cyber Exercise and Planning Program: Cyber Tabletop Exercise Package*, to aid in designing and facilitating cyber tabletop exercises.
- A copy of the *FLO Cybersecurity Toolkit* for fusion centers that are adding cyber to existing FLO programs.

DHS-001-05722-000135

REL0001269770

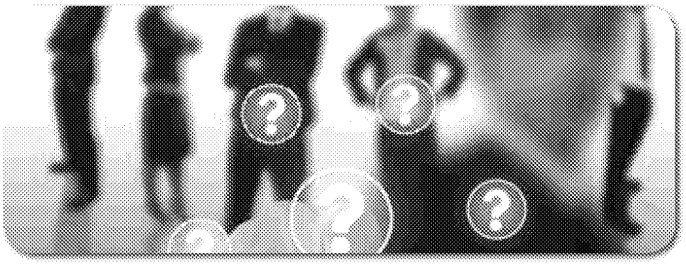
- A copy of the *Law Enforcement Cyber Incident Reporting* guide delineating the different ways in which law enforcement partners can report suspected or confirmed cyber incidents to federal partners.

The Toolkit is available to all fusion centers via the Homeland Security Information Network-Intelligence Community of Interest (HSIN-Intel), the HSIN Cyber Intelligence Network (CIN), and the Multi-State Information Sharing and Analysis Center (MS-ISAC).

DHS-001-05722-000136

REL0001269770

I. Fusion Process Capabilities



A. Fusion Center Operational Determination

To achieve the specific needs of the AOR, a fusion center should designate its operational focus on strategic analysis, technical analysis, tactical analysis, or a combination thereof.

- **Strategic analysis** assesses disparate bits of information to form integrated views on issues of national security and public safety and provide an overall picture of the intent and capabilities of malicious cyber actors; tools; and TTPs through the identification of trends, patterns, and emerging risks and threats.
- **Technical analysis** assesses specific, potential incidents related to investigations and events, provides specialized technical case and operational support, and produces highly technical intelligence, such as intelligence derived from forensic analysis and reverse engineering malware.
- **Tactical analysis** assesses specific, potential events and incidents related to near-term time frames and provides case and operational support, primarily in the form of raw information.

A fusion center that addresses both strategic and technical cyber analysis has the capability to provide strategic intelligence that focuses on the integration of international, national, and domain-specific intelligence with cross-programmatic issues pertinent to national security and public safety, as well as specialized case support and highly technical intelligence. The inclusion of tactical analysis allows a fusion center to support case development with resources and expertise that are not widely available.

B. Planning and Requirements Development

Intrastate Coordination

Fusion centers should partner with other fusion centers, FSLTT government agencies, and cyber stakeholders to develop and implement plans to coordinate cyber

The Toolkit contains cyber communication maps for strategic and technical fusion centers. The maps provide guidance for outreach efforts and indicate valuable points of contact and recommended information flows.

DHS-001-05722-000137

REL0001269770

information and intelligence sharing with regional cyber SMEs, in both the public and private sectors, and the cyber community. The plans should delineate who is responsible for disseminating what types of products and to whom. Other disseminators of cyber intelligence with overlapping AORs that may overlap with the fusion center's may include the state Homeland Security Advisor (HSA), Emergency Operations Centers (EOCs), Offices of the state Chief Information Officer (CIO) and the Chief Information Security Officer (CISO), and IT departments, as well as InfraGard, the Federal Bureau of Investigation's (FBI) Cyber Task Force (CTF), the U.S. Secret Service's (USSS) Electronic Crimes Task Force (ECTF), and local working groups. Collectors of cyber information and intelligence may include the IT departments of state, local, tribal, and territorial (SLTT) governments and the private sector, as well as academia, and cybersecurity researchers and organizations. [BC.I.A.1, page 12]

Information Sharing and Analysis Organizations (ISAO) and Information Sharing and Analysis Centers (ISACs)

Fusion centers should partner with ISAOs and ISACs, especially the MS-ISAC, to develop and implement plans to coordinate cyber information and intelligence sharing.

Risk Assessment

Fusion centers should collaborate with the cyber community to incorporate relevant IT, cybersecurity, and cybercrime information and analysis into statewide and/or regional risk assessments that identify and prioritize threats, vulnerabilities, and consequences to or within the AOR. [BC.I.A.2, page 12]

- Fusion centers should use available national and statewide risk assessments and other relevant products that identify patterns and trends reflective of emerging threats in the development of statewide and regional risk assessments. [BC.I.A.2.a, page 12]
- Fusion centers should partner with the cyber community to develop appropriate cyber risk assessments and share those risk assessments with officials and key stakeholders. [BC.I.A.2.b, c, page 12]
- Fusion centers should post all cyber analytic products to HSIN-Intel, in accordance with annual Homeland Security Grant Program requirements. [BC.I.A.2.d, page 12]

Information Requirements

Fusion centers should work with the cyber community to define, document, prioritize, and regularly update cyber-specific Standing Information Needs (SINs) for the center and the cyber community, inclusive of establishing goals and objectives for collecting, producing, and sharing information. [BC.I.A.3, page 13]

Suspicious Activity Reporting (SAR)

Fusion centers should develop, implement, and maintain plans to incorporate suspicious cyber activity and incident reporting, consistent with the *Law Enforcement Cyber Incident Reporting Unified Message*, the *SAR Unified Message*, and the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) SAR Data Repository (SDR), including the FBI's eGuardian program. [BC.I.A.4, page 13]

The Toolkit Organizations, Campaigns, Training, Resources, and Assessments document contains further information on many of the available resources that fusion centers can adopt and use to further cyber programs.

- Baseline Capabilities I.A.4.c.ii states that fusion centers should support the development of "outreach material for first responders, public safety, and private sector partners and the public to educate them on recognizing and reporting behaviors and incidents indicative of criminal activity associated with international and domestic terrorism." Fusion centers should extend this effort, along with advocating for the associated protection of privacy, civil rights, and civil liberties, through the Fusion Liaison Officer (FLO) program. Additional resources are available through ongoing cyber campaigns, including Stop. Think.Connect™ and National Cyber Security Awareness Month (NCSAM). [BC.I.A.4.c.ii, page 13]
- Some cyber SARs may include information relative to known international terrorist organizations or potential domestic terrorist or criminal issues. Fusion centers should determine

DHS-001-05722-000138

REL0001269770

whether these matters should be investigated as terrorism or only criminal matters based upon the following guidance:

- SARs with only a criminal nexus should be reported as cyber SARs consistent with the FBI's eGuardian program.
- SARs with a potential terrorism nexus and consistent with the behavioral criteria listed in the Information Sharing Environment-Suspicious Activity Reporting (ISE-SAR) Functional Standard should be submitted to the SDR as shared counterterrorism ISE-SARs.

- The term "cyber attack" is one of the 16 ISE-SAR behaviors outlined in the Functional Standard. The determination of whether a particular cyber SAR is linked to terrorism and subject to being shared via the SDR relies upon the analyst's application of NSI training on the review and submission of SAR in accordance with the Functional Standard and the SDR concept of operations (CONOPS). Consideration of the known actor(s), the targeted IT infrastructure and associated vulnerabilities, likely consequences, and historical background are all key to making such a determination.

- Fusion centers should use and promote federally provided outreach and training resources, such as the DHS Critical Infrastructure Cyber Community C³ Voluntary Program, DHS Cyber Information Sharing and Collaboration Program (CISCP), Enhanced Cybersecurity Services (ECS), Cyber Security Evaluation Program (CSEP), and the FBI's CyberShield. Fusion centers should also promote cybersecurity awareness campaigns, such as Stop. Think.Connect™ and National Cyber Security Awareness Month, to increase and magnify the cyber community's and citizens' awareness and magnify fusion center cyber resources. [BC.I.A.4.c.ii, f, pages 13–14]

Alerts, Warnings, and Notifications

Fusion centers should ensure that cyber alerts, warnings, and notifications are disseminated, as appropriate, to the cyber community and that those provided by the cyber community are disseminated, as appropriate, to the federal government. [BC.I.A.5, page 14]

Situational Awareness Reporting

Fusion centers should develop plans and processes to ensure that cyber alerts and warnings are reported to key officials and the public, as appropriate. [BC.I.A.6, page 14]

The MS-ISAC hosts threat and event alert-level maps, which are updated by state governments on a weekly basis and provide a common operational picture of the SLTT cyber alert and event levels. Access is available through the MS-ISAC.

Data Sources

Fusion centers should work with cyber stakeholders to identify and, if appropriate, request access to relevant cyber-related strategic, technical, and tactical data resources or systems. Recommended data sources include HSIN, MS-ISAC, the National Fusion Center Association's (NFCA) Cyber Threat Intelligence (CTI) group, CISCP, iGuardian, and the Internet Crime Complaint Center (IC3), as well as state ISACs and EOCs and private sector resources. Fusion centers should also ensure their data is made available to federal partners. [BC.I.A.7, page 14]

Coordination With Response and Recovery Officials

Fusion centers should work with cyber partners to ensure that information sharing and analysis capabilities of the centers are leveraged to support the response and recovery from cyber, criminal, and terrorism activity and natural disasters. In accordance with *Considerations for Fusion Center and Emergency Operations Center Coordination: Comprehensive Preparedness Guide* (CPG) 502 (May 2010), plans and procedures should be updated to include cyber roles, responsibilities, and mechanisms for sharing information and should be identified and communicated to all relevant stakeholders,

DHS-001-05722-000139

REL0001269770

including EOCs and emergency management agencies. [BC.I.A.8, page 14]

Information Sharing Coordination

Fusion centers should integrate cyber partners and/or, if necessary, develop, implement, and maintain plans and procedures for sharing information with cyber partners and stakeholders, CI owners and operators, and the private sector. Fusion centers should include in the plan the procedures to disseminate alerts, warnings, and notifications and other relevant analytic reports to CI sectors and/or private sector entities that are affected by or vulnerable to the threat. Fusion centers should determine their capability to assist during a cyber incident response and ensure that partners are aware of the fusion center's capability to assist. [BC.I.A.9, page 15]

Relevant exercises may include the national Cyber Storm and Cyber Guard exercises and local exercises hosted at the state and local level in response to specific incidents, events, or needs. Exercise play may be achieved by contacting the state CISO, the Homeland Security Advisor (HSA), the state Adjutant General (TAG), local National Guard offices, and MS-ISAC.

Exercises

Fusion centers should participate in exercises conducted by FSLTT and private sector organizations responsible for maintaining the cybersecurity of varying networks, in order to create a comprehensive public-private approach to cybersecurity preparation and readiness. In addition, fusion centers should include appropriate individuals from the cyber community in exercises designed to evaluate fusion center operations and information sharing processes. Fusion centers should work with cyber stakeholders to develop action plans to mitigate any gaps in collaboration efforts that are identified during these exercises. [BC.I.A.10, page 15]

C. Information Gathering/ Collection and Recognition of Indicators and Warnings

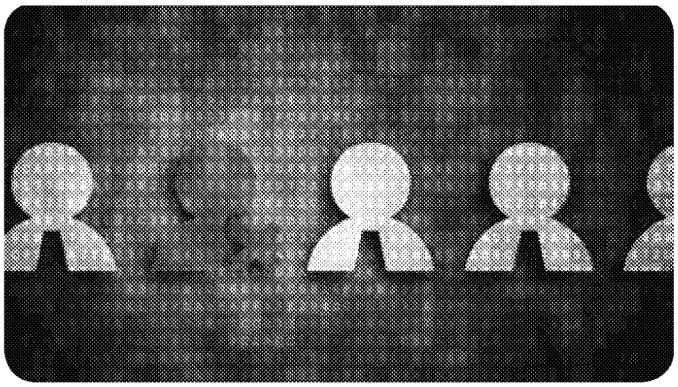
Information-Gathering and -Reporting Strategy

Fusion centers should develop, implement, and maintain an information-gathering and -reporting strategy that leverages existing capabilities and cyber partners and stakeholders. [BC.I.B.1, page 16]

- The strategy should include the FLO program, the MS-ISAC and other ISACs, national and local cyber working groups, CTF, ECTF, and InfraGard and clearly outline the collection process.
- If a local working group does not exist to bring together law enforcement and FSLTT government officials to discuss cyber matters, the fusion center should work to develop such a group.

Feedback Mechanism

Fusion centers should work with cyber partners and stakeholders to integrate feedback mechanisms for cyber information and intelligence, both provided and received, into existing feedback mechanisms. The feedback mechanism, ideally in the form of an anonymous survey, should allow partners to communicate the accuracy



DHS-001-05722-000140

REL0001269770

and value of the information and/or intelligence and the effectiveness of incorporating it and should also allow partners to make suggestions for improvement. [BC.I.B.2, page 16]

Collection and Storage of Information

In collaboration with cyber SMEs, fusion centers should identify the mechanisms for receiving, cataloging, retaining, and querying cyber information and intelligence at the centers in a manner that is consistent with the centers' privacy, civil rights, and civil liberties protections. Cyber information should include indicators of compromise (IOC), IP addresses, domains, aliases, and file hashes. [BC.I.B.3, page 16]

- Jurisdictions have established legislation and practices reflecting case law that determine how information may be gathered and what information may be obtained before it is considered an unreasonable search and seizure as protected by the Fourth Amendment of the U.S. Constitution. Collection and storage of intelligence information should be maintained in accordance with all applicable laws regarding privacy, civil liberties, search and seizure, and 28 CFR Part 23.

- Fusion centers should work with local CIOs and CISOs responsible for the fusion centers' network operations to facilitate the receipt, sharing, and querying of cyber information and intelligence.

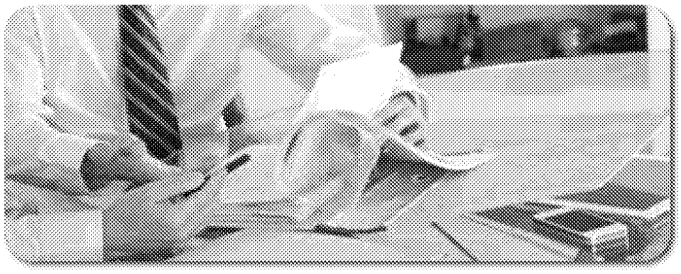
- Fusion centers should, if applicable, be knowledgeable of local laws and regulations regarding the search and seizure of cyber information, as well as evidentiary handling.

- Cyber information may contain personally identifiable information (PII); protected health information (PHI); protected critical infrastructure information (PCII); confidential business information; information with classification markings, dissemination caveats, or Traffic Light Protocol (TLP) markings (https://www.us-cert.gov/tlp) (see Appendix B); or other sensitive and/or protected information.

- Fusion centers should work with DHS's National Cybersecurity and Communications Integration Center (NCCIC), the U.S. Computer Emergency Readiness Team (US-CERT), and the MS-ISAC to facilitate the receipt, sharing, and querying of cyber information and intelligence.

The Toolkit contains additional information on STIX, TAXII, and Cyber Observable eXpression (CybOX).

- Fusion centers should work with relevant FSLTT and private sector cyber partners and stakeholders to eventually develop the ability to share, process, and analyze cyber information at machine speed. This should be accomplished through fusion center compliance and use of accepted standards for exchanging information, including the use of the National Information Exchange Model (NIEM), Structured Threat Information eXpression (STIX) language, and Trusted Automated eXchange of Indicator Information (TAXII), as applicable.



D. Processing and Collation of Information

Information Collation and Levels of Confidence

Fusion centers should collaborate with cyber partners and use the necessary tools to process and collate cyberthreat information, indicators, warnings, or suspicious activity and ensure that cyberthreat information, indicators, or warnings are relevant, valid, and reliable. [BC.I.C.1, 2, page 17]

- Fusion centers should leverage existing levels of confidence and standardize cyber risk and impact levels to ensure consistency among cyber information and intelligence production.

The Toolkit contains standardized cyber risk and impact-level language.

DHS-001-05722-000141

REL0001269770

E. Intelligence Analysis and Production

Analytic Products

Fusion centers should update their production plans to incorporate cyber-related analysis and work with cyber partners and stakeholders to develop any relevant, new cyber products. These may include strategic, technical, and/or tactical cyber information and intelligence. Fusion centers should also update their production plans to incorporate cyber-related analysis into products pertaining to other subject areas. [BC.I.D.1, page 18]

Information Linking

Analysts and investigators focused on cyber matters should work in partnership with other fusion centers and partner agencies to understand and identify links between cyber actors, TTPs, indicators, patterns and trends, and terrorism and criminal information or targeting, particularly targeting of CI and key sectors. [BC.I.D.4, page 19]

Strategic Analysis Services

Fusion centers should provide strategic analysis for the AOR served, whether they elect to perform as technical cyber fusion centers or as strategic cyber fusion centers. [BC.I.D.5, page 19]

Open Source Analysis Capability

Fusion centers should make use of open source cyber information and intelligence, including white papers, quarterly and annual cybersecurity reports, news articles, data dumps, and reporting by threat actors. [BC.I.D.6, page 19]

Analyst Specialization

Fusion centers should consider allowing analysts and officers to specialize in cyber information and intelligence and consider the implementation of strategic, technical, and/or tactical cyber Intelligence Analysis positions. [BC.I.D.7, page 19]

Analytic Tools

Fusion center analysts and investigators focused on cyber issues should have the necessary tools for the analysis of cyber information and data. These tools include those resources outlined in Global's *Analyst Toolbox*, as well as those resources and tools described in the *Fusion Center Cyber Toolkit*. [BC.I.D.8, page 19]

The Fusion Center Guidelines document states that "analysis transforms the raw data into products that are useful . . . the goal is to develop a report that connects information in a logical and meaningful manner to produce an intelligence report that contains valid judgments based on analyzed information." One of the primary goals of a fusion center cyber program should be to develop cyber intelligence that key decision makers, who are not well-versed in cyber matters, can understand and use to determine future courses of action. The use of a feedback mechanism allows the fusion center to evaluate and adjust intelligence dissemination in order to better meet this goal.

DHS-001-05722-000142

REL0001269770

F. Intelligence and Information Dissemination

Dissemination Plan

Fusion centers should incorporate cyber stakeholders into their existing dissemination plans. Such plans should document the types of cyber-specific products to distribute to the cyber community, the procedures for doing so, and the appropriate mechanisms. [BC.I.E.1, page 20]

- Fusion centers should create independent communication paths for cyber information and intelligence, consistent with classification markings, dissemination caveats, and TLP levels.
- Fusion centers should endeavor to produce information and intelligence products at the lowest possible classification and dissemination level, in order to share the products as widely as possible.
- Cyber partners should collaborate with fusion centers to identify appropriate members of the cyber community to include in the centers' dissemination of information and intelligence marked with a classification, dissemination, or TLP level.
- Fusion centers should include the cyber community in the dissemination lists for noncyber products with possible cyber implications, to enable the cyber community to readily assist with incident response and mitigation efforts.

Reporting of Information to FSLTT Partners

Fusion centers should ensure that relevant cyber information or intelligence products are shared with appropriate federal agencies—such as the DHS Office of Intelligence and Analysis (I&A), the NCCIC, and the FBI—as well as posted to HSIN-Intel, and shared with other fusion centers and ISAOs, including the MS-ISAC. [BC.I.E.3, page 20]

- Relevant cyber information should be coordinated through DHS and/or the FBI to develop Intelligence Information Reports (IIRs) for sharing with the U.S. Intelligence Community (IC).
- To facilitate analyst-to-analyst exchange, fusion centers should utilize HSIN, the MS-ISAC, and the CTI, as well as local working groups.

G. Reevaluation

Fusion Center Processes Review

Fusion centers should consider the rapidly changing cyberthreat environment when reevaluating their plans to update information requirements, collection plans, and analytic production strategies and determine whether a more rapid review is necessary. [BC.I.F.2, page 21]

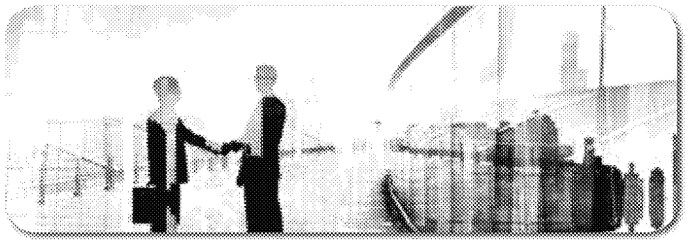
DHS-001-05722-000143

REL0001269770

DHS-001-05722-000144

REL0001269770

II. Management and Administrative Capabilities



A. Management and Governance

Governance Structure

Fusion centers should consider the addition of a cyber representative into the centers' governance structure. [BC.II.A.1, page 23]

- Inclusion of the state and/or major urban area CIO and CISO is recommended.

Mission Statement

Fusion centers should review and update their mission statements, if appropriate, to ensure that the statements convey the purpose, priorities, and roles of the centers as they pertain to cyber-related activities. [BC.II.A.2, page 24]

Collaborative Environment

Fusion centers should work with the cyber community to identify cyber partners, stakeholders, and the community at large; develop the roles and responsibilities of each; and implement mechanisms and processes to facilitate collaboration. Mechanisms and processes may include a need to adjust or develop a Memorandum of Understanding (MOU) or Agreement (MOA) or Nondisclosure Agreement (NDA) between each center and each participating cyber organization to help define collaborative efforts, such as resources or personnel, and ensure understanding of all relevant information privacy, civil rights, and civil liberties protections. [BC.II.A.3, page 25]

Policies and Procedures Review

Fusion centers should review and update their policies and procedures manuals to reflect the incorporation of cyber goals and policies and outline the roles and responsibilities of cyber entities that are involved in the centers, including privacy policies, security policies, and center directives. [BC.II.A.4, page 26]

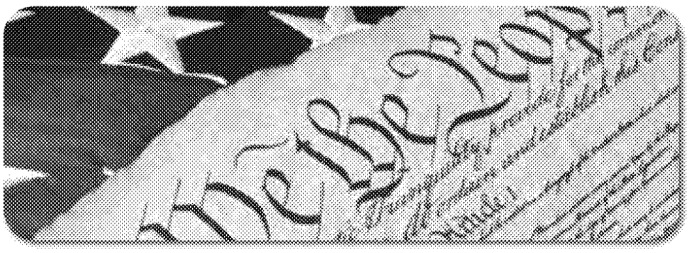
Fusion centers' security policies should address the need, if applicable, to collect, store, and share malware, malicious code, and other indicators that may cause harm when transmitted or stored through standard mechanisms and techniques, inclusive of sharing with US-CERT, the MS-ISAC, SLTT CISOs, cyber stakeholders, and the FBI's Malware Investigator platform. The intake function for potential harmful indicators should be separate from the intake function for nonharmful information.

Outreach

Fusion centers should build relationships with cyber partners, stakeholders, and SMEs to provide outreach and communications to leaders, policymakers, and CI owners and operators regarding cyber resources and capabilities available to them, the fusion process, the intelligence cycle, the types of information to be shared with the fusion center, and mechanisms to report this information. [BC.II.A.6, page 26]

DHS-001-05722-000145

REL0001269770



B. Information Privacy Protections

Privacy Policy Review, Implementation, and Audit

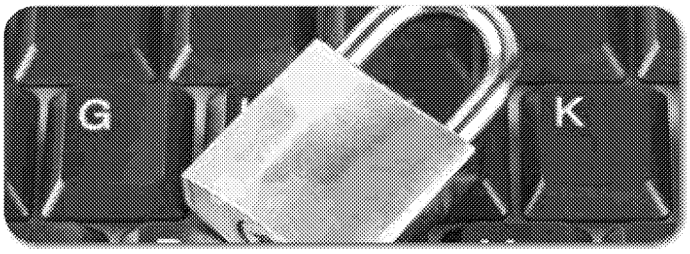
Fusion centers should incorporate cyber partners into the review, implementation, and audit of privacy policies that address gathering, analysis, and dissemination of protected or sensitive cyber information and other proprietary or personally identifiable information, as appropriate.

Privacy Protections

Fusion centers should collaborate with cyber partners to ensure the incorporation of cyber-related information and analysis into their operations in a manner that protects privacy, civil rights, and civil liberties in accordance with the centers' privacy, civil rights, and civil liberties protections and all applicable laws.

Privacy Policy Outreach

Fusion centers should work with cyber partners to develop and implement the necessary outreach and training to ensure appropriate privacy, civil rights, and civil liberties protections for cyber information. Cyber stakeholders and fusion center personnel should participate in ongoing and regular training. Cyber partners should participate in available privacy, civil rights, and civil liberties trainings, including training on 28 CFR Part 23, to ensure compliance with fusion center privacy, civil rights, and civil liberties policies and procedures, including social media policies.

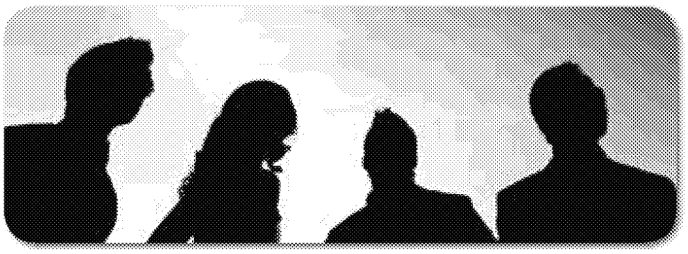


C. Security

Security Measures

Fusion centers should ensure that their security policies allow for the timely distribution of information and intelligence products to the center's cyber stakeholders, including the use of automated mechanisms to disseminate IOCs. [BC.II.C.3.d, page 31]

Baseline Capabilities II.D.3.c.i states that "all fusion center personnel—including analysts, intelligence officers, and non-law enforcement personnel assigned to the center (corrections, fire services, public health, private sector, and others)—assigned both full-time, part-time, and on an 'as needed' basis should be included in the training plan."



D. Personnel and Training

Staffing and Training Plan

Fusion centers should develop and document staffing plans that support the incorporation of cyber personnel into the fusion centers or define mechanisms to utilize cyber subject-matter support from personnel who do not staff the fusion centers. Because of the unique and complex nature of cyber activity, fusion centers should assign at least one analyst to cover cyber matters on

DHS-001-05722-000146

REL0001269770

at least a part-time basis. Should fusion center cyber responsibilities expand, each fusion center should consider assigning or bringing in partner analysts and cyber SMEs from the local cyber community to focus on particular cyber specializations, as required by the fusion center's priorities, and/or to provide general subject-matter expertise. [BC.II.D.1, 3, pages 31–32]

- Fusion centers should ensure that training plans incorporate a base level of cyber awareness for all employees.
- Fusion centers should consider facilitating sponsorship of clearances for appropriate cyber partners, including CIOs, CISOs, and other cyber stakeholders, to facilitate analytic efforts and data exchange.

Fusion Process Management

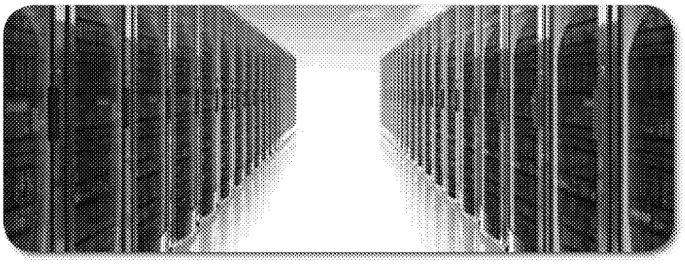
The intelligence manager position should be updated to incorporate the addition of a cyber program into the fusion center. [BC.I.D.2, page 18]

Enhancing Analyst Skills

Fusion centers should develop and implement a Training and Professional Development Plan that provides cyber analysts, sworn investigators, managers, and others in the chain of command with the appropriate KSAs to handle cyber matters, inclusive of the topics outlined in the Toolkit Cyber Intelligence Analyst Basic Skill Set and the Toolkit Recommended Career Paths documents. Recommended topics include basic computer, networking, security, and communication knowledge, along with knowledge of cyber actors and TTPs. [BC.I.D.3, page 19]

- Fusion centers should include internships and mentoring partnerships with local and national SMEs to allow cyber analysts to gain the requisite KSAs to work cyber matters.
- Analysts and investigators focused on cyber topics should be trained in all relevant analytic and information protection regulations, procedures, and considerations to ensure that cyber information, as well as the information contained within the cyber data, is appropriately gathered, processed, analyzed, disseminated, protected, and secured.

The Toolkit contains documents that outline the Cyber Intelligence Analyst Basic Skill Set and the Recommended Career Paths, which provide additional guidance in developing fusion center cyber roles and knowledge, skills, and abilities. In addition, it contains template job descriptions for a Tactical Fusion Center All Source Cyber Intelligence Analyst, Technical Fusion Center Cyber All Source Intelligence Analyst, Strategic Fusion Center Cyber All Source Intelligence Analyst, Fusion Center Supervisory Cyber Intelligence Analyst, and Fusion Center Cyber Investigator.



E. Information Technology/ Communications Infrastructure, Systems, Equipment, Facility, and Physical Infrastructure

Information Exchange Within the Fusion Center

Fusion centers should work with cyber partners to ensure that the appropriate technological and physical solutions are incorporated to allow for the appropriate integration of cyber interests into the center's operations. [BC.II.E.2, page 33]

- Fusion centers' technological solutions should address the need, if applicable, to collect, store, and share malware, malicious code, and other

DHS-001-05722-000147

REL0001269770

indicators that may cause harm when transmitted or stored through standard mechanisms and techniques, inclusive of sharing with sharing with US-CERT, the MS-ISAC, SLTT CISOs, cyber stakeholders, and the FBI's Malware Investigator platform. Fusion centers should work with their network owners and operators to ensure that the intake function for potential harmful indicators is separate from the intake function for nonharmful information.

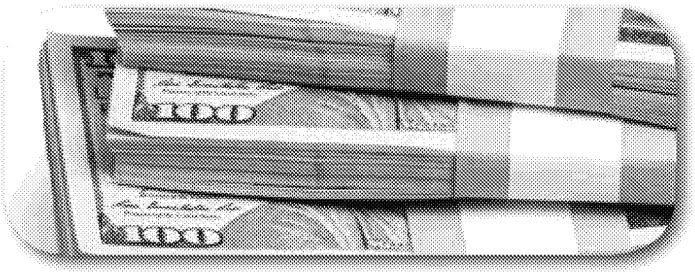
- Cyber stakeholders should identify and inform the fusion center of relevant databases, systems, and networks available from cyber FSLTT and private sector organizations to maximize information sharing and analysis that relate to cyber information. [BC.II.E.2.b, page 33]

Communications Plan

Fusion centers should collaborate with cyber partners to identify how they will communicate during an incident or emergency, especially those requiring cyber expertise, and ensure that communication capabilities are interoperable. [BC.II.E.3.a, page 33]

Contingency and Continuity of Operations Plans

Fusion centers should review and update contingency and continuity of operations plans to support the incorporation of cyber-related duties and responsibilities. [BC.II.E.4, page 33]



F. Funding

Fusion centers should work with the cyber community to develop a funding strategy, leverage existing resources, and identify supplemental funding sources to support the integration of cyber personnel and information into fusion center operations. [BC.II.F.1.d, page 34]

DHS-001-05722-000148

REL0001269770

Appendix A: Acronyms

AOR	Area of Responsibility
Baseline Capabilities	*Baseline Capabilities for State and Major Urban Area Fusion Centers*
BJA	Bureau of Justice Assistance
CI	Critical Infrastructure
CIN	Cyber Intelligence Network
CIO	Chief Information Officer
CISCP	DHS Cyber Information Sharing and Collaboration Program
CISO	Chief Information Security Officer
COI	Community of Interest
CONOPS	Concept of Operations
CPG	Comprehensive Preparedness Guide
CSEP	Cyber Security Evaluation Program
CTF	Cyber Task Force
CTI	Cyber Threat Intelligence
Cyber	Information Technology, Cybersecurity, Cybercrime
CybOX	Cyber Observable eXpression
DHS	U.S. Department of Homeland Security
ECS	Enhanced Cybersecurity Services
ECTF	Electronic Crimes Task Force
EOC	Emergency Operations Center
FBI	Federal Bureau of Investigation
FLO	Fusion Liaison Officer
FSLTT	Federal, State, Local, Tribal, Territorial
GAC	Global Advisory Committee
Global	Global Justice Information Sharing Initiative
HSA	Homeland Security Advisor
HSIN	Homeland Security Information Network
HSIN-Intel	Homeland Security Information Network-Intellligence
HSEC SIN	Homeland Security Standing Information Need
I&A	DHS Office of Intelligence and Analysis
IC	Intelligence Community
IC3	Internet Crime Complaint Center
ICS	Industrial Control Systems
IIR	Intelligence Information Reports
IOC	Indicators of Compromise
IP	Internet Protocol
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization
ISE-SAR	Information Sharing Environment-Suspicious Activity Reporting
ISP	Internet Service Provider
IT	Information Technology
KSA	Knowledge, Skill, and Ability
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MS-ISAC	Multi-State Information Sharing and Analysis Center
NCCIC	National Cybersecurity and Communications Integration Center
NCSAM	National Cyber Security Awareness Month
NDA	Nondisclosure Agreement
NFCA	National Fusion Center Association
NIEM	National Information Exchange Model
NIST	National Institute of Standards and Technology

DHS-001-05722-000149

REL0001269770

NSI	Nationwide SAR Initiative
PCII	Protected Critical Infrastructure Information
PHI	Protected Health Information
PII	Personally Identifiable Information
SAR	Suspicious Activity Report
SDR	SAR Data Repository
SIN	Standing Information Need
SLTT	State, Local, Tribal, and Territorial
SME	Subject-Matter Expert
STIX	Structured Threat Information eXpression
TAG	The Adjutant General
TAXII	Trusted Automated Exchange of Indicator Information
TLP	Traffic Light Protocol
TTPs	Tactics, Techniques, and Procedures
U.S.	United States
US-CERT	United States Computer Emergency Readiness Team
USSS	United States Secret Service

DHS-001-05722-000150

REL0001269770

Appendix B: Traffic Light Protocol

Traffic Light Protocol (TLP) is a set of designations used to ensure that sensitive information is shared with the correct audience. It employs four colors to indicate different degrees of sensitivity and the corresponding sharing considerations to be applied by the recipient(s). https://www.us-cert.gov/tlp

Color	When should it be used?	How may it be shared?
RED	Sources may use TLP: RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.
AMBER	Sources may use TLP: AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may share TLP: AMBER information only with members of their own organization who need to know and only as widely as necessary to act on that information.
GREEN	Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.
WHITE	Sources may use TLP: WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	TLP: WHITE information may be distributed without restriction, subject to copyright controls.

DHS-001-05722-000151

REL0001269770

DHS-001-05722-000152

REL0001269770

Appendix C: Cyber Incident Severity Schema

Version 1.0

Incident Level and Coordination

Significant Incidents ↑

	General Definition	Handling Precedence	
		Interagency Coordination	Targeted Entity Contact[iii]
Level 5 Emergency (Black)[ii]	Poses an imminent threat to the provision of wide-scale critical infrastructure services, national government stability, or the lives of U.S. persons.	Immediate. An appropriate agency will initiate ECAP conferencing procedures.	If relevant and as needed.
Level 4 Severe (Red)	Likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties.	Immediate. Elevate to the CRG[ix] for rapid consultation; possible initiation of ECAP[x] Convene UCG[xi] and C- CAR,[xii] as appropriate.	Immediate
Level 3 High (Orange)	Likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.[xiii]	Begin coordination within 1 hour. Elevate to the CRG for its awareness and deliberation. Convene UCG and C-CAR, as appropriate.	Initiate contact within 8 hours; in-person response within 24 hours.
Level 2 Medium (Yellow)	May impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	Begin coordination within 4 hours.	Initiate contact within 24 hours; in-person response within 5 days.
Level 1 Low (Green)	Unlikely to impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	Discretionary	Discretionary[xiv]
Level 0 Baseline (White)	Unsubstantiated or inconsequential event.	Not warranted	Not warranted

Level 1 through 4 incidents will be ticketed in the E.O. 13636 Section 4(b) system.

DHS-001-05722-000153

REL0001269770

Factors to Consider When Assigning a Severity Level[i]

Who…	did what…	to whom…	and why?	
Significance of Threat Actor	**Observed Actions[iv]**	**Targeted Entity Criticality**	**Intended Consequence[v]**	**Potential to Impact Foreign Relations[ii]**
High	Effect	Section 9 CIKR entity, essential government capability, or significant special event (NSSE[viii] or SEAR-1)	Cause physical consequence	A dramatic change in another nation's intentions or capabilities.
			Damage computer and networking hardware	
	Presence	Other CIKR entity, key government capability, or large public event (SEAR-2 to -4)	Corrupt or destroy data	Activity that may undermine an impending diplomatic engagement or sensitive negotiation.
See Cyber Threat Actor Grouping product[vii]			Deny availability to a key system or service	
	Engagement	An otherwise significant entity	Steal sensitive information	Compromise of information from a U.S. system that harms foreign relations.
			Commit a financial crime	Compromise of U.S. information from an ally/ partner system.
Low	Preparation	Small business or individual	Nuisance DoS or defacement	

Purpose and Scope

This schema will support and inform interagency coordination efforts by the Cyber Centers, departments and agencies with a cyber mission, and the National Security Council (PPD-1) system. It is not a substitute for procedures employed by individual departments and agencies that are tailored to their unique roles in cyber incident management. This schema will serve two purposes:

- Inform the time urgency and seniority level at which coordination efforts are required; and
- Inform the time urgency and level of investment required of response efforts

Given the frequency of information gaps concerning cyber threats, the general expectation is that departments and agencies will make every effort to render a timely and reliable assessment based on the available information.

DHS-001-05722-000154

REL0001269770

Appendix C Footnotes

i These factors are generally listed from greatest significance (top) to least (bottom), but are not exhaustive or strictly tethered to the severity levels in the table on the left. An incident handler must consider the totality of the known circumstances and tag the incident based on the general definitions. The tag will be updated as new facts are learned.

ii A watch officer will rarely be able to assess an incident's potential impact on foreign relations. Typically, a regional subject matter expert or policymaker will assess this factor upon their review of the incident.

iii As defined and described in the document entitled, *Process for Dissemination of Cyber Threat Information to Specific Targeted Critical Infrastructure Entities*, accepted on June 6, 2014. The clock for targeted entity contact (aka, "victim notification") begins when coordination is completed and a course of action is agreed to.

iv See the ODNI Cyber Threat Framework taxonomy.

v In addition to characterizing the observed activity, one must consider the scope and scale of the incident when applying the general definitions to arrive at a severity level.

vi A decision to escalate an incident to Level 5 requires the recommendation of a senior officer (e.g., an Interagency Policy Committee or CRG representative).

vii Reference the *Cyber Threat Actor Grouping* product, co-developed and maintained by the National Cyber Investigative Joint Task Force (NCIJTF) and ODNI.

viii The U.S. Secret Service should be notified of threats to a National Security Special Event (NSSE), or threats to entities supporting it.

ix The Cyber Response Group (CRG) is a standing body comprised of the cyber center directors and policymakers who oversee cyber threat and incident management efforts and expeditiously resolve policy issues that arise as a result of them. The CRG is chaired by the National Security Council (NSC) Cybersecurity Directorate.

x Emergency Cyber Action Procedures (ECAP).

xi The Cyber Unified Coordination Group (UCG) is a standing body of representatives from the U.S. Government and the private sector to synchronize efforts to identify, protect against, detect, respond, and recover from significant cyber incidents. The National Cybersecurity and Communications Integration Center (NCCIC) serves as the UCG's executive secretariat.

xii The Federal Cybersecurity Coordination, Assessment, and Response (C-CAR) protocol allows DHS, through the NCCIC, to convene federal department and agency CIOs and CISOs on significant cybersecurity issues that may affect U.S. Government information systems.

xiii Reference is made to the description of *Public Confidence* contained in HSPD-7: "Terrorists seek to destroy, incapacitate, or exploit critical infrastructure and key resources across the United States to threaten national security, cause mass casualties, weaken our economy, and damage public morale and confidence," and "… undermine the public's morale and confidence in our national economic and political institutions." HSPD-7's call to ensure that the public's trust and confidence are not damaged by the actions of terrorists can also be applied to cyber incident management efforts.

xiv Targeted entity contact might be deferred if the information is deemed to be of low confidence or not of a level of specificity that would allow the entity to take action.

DHS-001-05722-000155

REL0001269770

REL0001269770