Virginia
Area Contingency Plan
(VACP)

Information Management Annex

Annex KK
March 2025

Table of Contents

1000 – Introduction

An Information Management Plan (IMP) should be developed at the beginning of response operations and planned events. The IMP establishes the framework for information management and data sharing across the response action. Information management relates to the tasks of collection, processing, situation displays, storage, distribution, and protection of data and information. This annex serves as a resource for developing an Information Management Plan and serves as a complement to the USCG Incident Management Handbook (IMH).[1]

1100 – Principles

The following principles form the foundation for the management and use of information within the Incident Command System (ICS) organization:

- Information is an asset that has value to the IC/UC and should be managed accordingly.
- Information is accessible and is shared across the organization to increase knowledge and understanding and improve the effectiveness of response operations.
- Adequate personnel, equipment and funding resources are provided to ensure information is managed properly.
- Data and information are defined consistently throughout the ICS organization, and the definitions are understandable and available to all response personnel.
- Data and information is secure and protected from unauthorized access, use and disclosure and managed in accordance with the guidelines set out in the below sections.

1200 – Applicability

This annex applies to the management of all information, in any format or media that is created, received, stored and managed for final disposition for each event. The size and scope of the incident will determine whether a formal Information Management Plan is required. A full-blown Information Management Plan is typically developed during incidents that involve a significant number of Critical Information Requirements (CIRs), substantial media/political involvement, and/or complex information processing. Regardless of whether a formal Information Management Plan is developed, each area of information management covered in this annex should be addressed by the plan developers.

1300 – Legal Obligation to Preserve

During response operations and planned events, the IC/UC has a legal obligation to preserve relevant documents, electronically stored information (ESI), and physical evidence. This obligation is strict. Failure to preserve and retain documents and ESI may result in sanctions against the USCG and other response organizations. If you are unsure whether certain documents and ESI should be preserved, retain it until you have spoken to USCG legal counsel.

1400 – Definitions

Critical Information Requirements (CIRs) are a comprehensive list of information requirements that the IC/UC has identified as critical to facilitate timely decision making.

Essential Elements of Information (EEIs) are subsets of a CIR which provide greater detail on the information needed to meet the CIR.

Data is the rawest form of information as it has not yet been confirmed or evaluated against other data. Data may come from a wide variety of inputs, including operational assets, eyewitness reports, field observations, social media, and weather reports.

Information is created when data is assembled, organized and verified to develop a clear picture. Information constantly evolves as more data is added and the picture becomes clearer. Information sharing is what keeps everyone on the same page.

Intelligence is the result of analyzing information and adding findings, conclusions, and recommendations for actions.

2000 – Information Acquisition

Data and information inputs for a response action can come from a variety of sources:

- Observations of the spill by response personnel
- Base maps, reference layers, sensitivity indices
- Government and facility response plans
- Meteorological data sources
- NOAA trajectory models
- Social media monitoring
- Personnel, equipment and other resource tracking
- ICS plans and forms

2100 - Metadata

The IMP should identify all of the data, records and documents that are expected to be received and/or produced during the response action or planned event. After developing a comprehensive inventory of information, the IMP should a) describe the method for logging incoming data/information and b) define the metadata elements for data sets, records and documents, including:

- brief description
- ownership
- storage medium
- date of creation
- source
- usage
- target audience
- target date for archival/disposition

A table may be developed to display the type of information with its associated metadata elements.

For electronic files, the IMP should define the methodology used to name files (including databases, applications, documents and records).

2200 – Standardization & Quality Assurance/Control

Once received and properly logged, information will need to be evaluated for the following:

- Determine if data/information is related to the response action or planned event.
- Determine if data/information is valid or needs to be validated/verified.

The IMP should establish a QA/QC process before sharing data and information on situational displays.

3000 – Information Assurance

3100 – Information Delivery Platforms

Throughout a response operation, the IC/UC uses tools that include information management systems and various software tools used to put data, information and intelligence into organized frameworks. Information management tools are anything that is used to share and preserve information. The mission determines the tool. Commonly used tools include the information delivery platforms identified in Table 3-1. The IC/UC will need to determine which tool will be used for the response action or planned event.

Table 3-1. - Delivery Platforms

PLATFORM	PROS	CONS
Homeland Security Information Network (HSIN)	• Secure network approved for use by all DHS • Designed by DHS to remedy information sharing shortfalls • Designed similarly to SharePoint • Unlimited storage capacity for files • Unlimited number of users, good for large scale and long incidents • Can preload documents and plans	• All users require a username and password • Users must log in and change password every 90 days • Port stakeholders must be nominated to a community of interest by a DHS employee/Help Desk • Limited to the size of file that can be uploaded • Must have one person dedicated to managing HSIN during the response/exercise and enforce naming conventions
HSIN Adobe Connect	• Secure network approved for use by all DHS • Designed by DHS to remedy information sharing shortfalls • Port stakeholders can enter Adobe Connect as a guest • User friendly platform with the Meeting Host to limit Participant capabilities • Recommended for incidents less than 50 responders in ICP • Can preload documents and plans • Training available online	• Meeting hosts require an active HSIN username and password • Meeting hosts must log in and change password every 90 days • Limited to the size of file that can be uploaded • Must have one person dedicated to managing HSIN during the response/exercise and enforce naming conventions
APAN (Currently being beta-tested by Sector Virginia)	• Full SharePoint Capability • Can integrate full Adobe Connect Capability • All ICS documents available for use and collaborate in real-time • Can use to host meetings online • Can preload documents and plans	• Password must be updated regularly • Access to site must be approved by the site owner; only one allowed at a time. • Slight learning curve; will be improved with further beta-testing
Outlook Distribution Lists	• Ideal for very small incidents where decision makers and responders are not working side by side • Once emails are sent, there is an automatic log of events is created	• Unable to limit distribution of information once email update is sent
SharePoint	• Must be granted access or have ability to log into company/agency computer network	• USCG has stringent information technology standards and will have to determine if a company or agency's standards meet USCG standards. USCG personnel are not allowed to upload incident documents to sites outside of the USCG domain
WebEOC	• User friendly and an administrator can easily give people access • Roles based, which could limit access to information • Good for large incidents and responses • Platform being utilized by local, Commonwealth and FEMA • In person training required prior to access being granted • Commonwealth Common Operations Picture • Can add attachments • Can preload documents and plans • Unlimited number of users at one time • Web based	• Username and password; must be changed and updated regularly • Roles based, which could limit access to information

3200 – Access & Security

Information must be easily and conveniently accessible with appropriate controls in place to:

- Ensure access is authorized.
- Protect sensitive information.
- Protect against unauthorized modifications and disclosure.

Provisions must be made to ensure that the integrity of information is not lost or compromised through accident, error, or malicious intent and that access is not inhibited through denial of service or other attacks. Where certain information is sensitive in nature, the information may be made available for access in alternate formats and through channels that are responsive to user's needs.

The IMP should address the following access and security issues:

- Define security requirements and access rights in terms of who has access to information what information and for what purposes.
- Define where and how to get the information, including the necessary workflow.
- Define data integrity measures and mitigation.
- Define recovery measures in the event of accident, service denial, attack or other.

4000 – Information Distribution

4100 – Data Sharing Agreements

During a response action or planned event, the federal and state governments and the responsible party may utilize different delivery platforms or situational displays. Additionally, various information technology security requirements can limit information flow or access to users outside of an organization, requiring more than one situation display. To ensure continuity of data and information among all the response participants, the IMP should contain a "Data Sharing Agreement." The Agreement should consider data governance issues and subsequent requests for release of information.

4200 - ICS Roles for Information Managers

At the outset of response operation or planned event, the IC/UC need to identify and exercise an information management team within the Planning Section. These roles should be staffed in the first 24-48 hours with highly skilled interagency and RP personnel as data and GIS managers with experience in ICS and response needs.

The following positions within the ICS structure have information management responsibilities. The IC/UC may elect to add additional positions to support information management functions as the type and size of incident dictate.

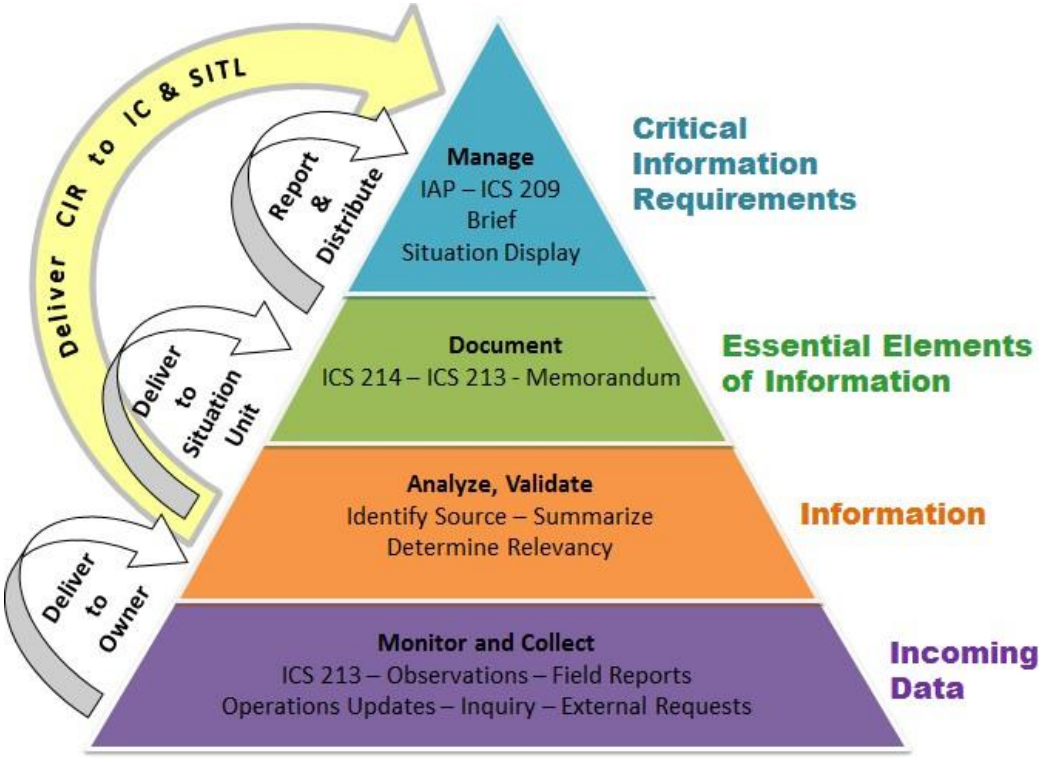
- The **Planning Section Chief (PSC)** is a member of the General Staff and responsible for the development of the IAP, the collection, evaluation, dissemination, and use of incident information and maintaining status of assigned and demobilized resources.

- The **Situation Unit Leader (SITL)** is the primary node for information management, which may include both unclassified and classified information. The SITL is responsible for collecting, processing, organizing and disseminating incident information relating to status of current operations, incident growth, mitigation, or intelligence activities taking place on the incident. The SITL may prepare future projections of incident growth, maps, and intelligence.

- The **Documentation Unit Leader (DOCL)** is responsible for the maintenance of accurate, up-to-date incident documentation which is critical to post-incident analysis. Examples of incident documentation include IAP(s), incident reports, communication logs, injury claims, and situation status reports. The Documentation Unit will store incident files for legal, analytical, and historical purposes in accordance with the standards.

4300 – Information Flow

Figure 4-1. – Information Flow



5000 – Information Disposition

- How do you handle it when it's no longer necessary?
- How do you determine what to destroy vs archive
- What legal obligations do you have that govern retention or destruction?
- What methods are used to destroy and ensure it can't be reconstituted?
- What methods are used to archive and protect it?

Appendix A
Sample Information Management Plan

1.0 Information Types

1.1 CIRs

1.2 EEIs

1.3 Information & Data

1.4 File Naming Conventions

1.4.1. Electronic documents

1.4.2. Digital photographs

Digital photographs shall be uploaded to the incident response photo log, located with the Documentation Unit. Photos shall be named in accordance with the prescribed standard naming convention outlined below.

LAST NAME_SECTION_LOCATION_DATE_LETTER
SMITH_OPS_XXX_07092025_A
SMITH_OPS_XXX_07092025_B

a) Photographer's last name
b) ICS section assigned
c) Geographic location photo was taken (e.g. segment or waterway)
d) Date photo was taken. Year, month, day (e.g. 20250309 = March 9, 2025)
e) Multiple photos from the same date and location will be differentiated with an alpha designator. (e.g. photo 1=A, photo 2=B, » » photo 27=AA)

2.0 Data Quality Assurance/Control

3.0 Delivery Platforms

Table 1. – Information Metadata

	Brief Description	Ownership	Storage Medium	Source	Usage	Target Audience	Date for Archival
Observations of the spill by response personnel							
Base maps, reference layers, sensitivity indices							
Government and facility response plans							
Meteorological data sources							
NOAA trajectory models							
Social media monitoring							
Personnel, equipment and other resource tracking							
ICS plans and forms							
Photographs							

Table 2. – Ownership

Information Management Ownership Crosswalk									
	TASKING	CIR DEVELOPMENT	GATHERING	VERIFY, SYNTHESIZE & ANALYZE	VALIDATION & AUTHORIZATION	DISSIMENATION – Internal	DISSIMENATION – External	CUSTOMER OR USER	
IC/UC	P	P	X		P	X	P	P	
PIO		X	X	X	X		Media	P	
LOFR		X	X	X	X	X	Stakeholders	P	
SOFR			X						
OSC Operations Section Chief	X	P	X	X		P		P	
ISC	X	P	X	X	X	P	Intelligence & Investigation Community	P	
PSC	X					X	X		Plan Manager
SITL			X	P	X	P			Plan Developer
MTSL			X	P	X		MTSL Community	P	
RESL			X	X		X			
LSC		X	X	X			LSC Community	P	
COML			X	P	X				
FSC			X	X			FSC Community	P	

P = Primary Role
X = Supporting Role

Table 3. Information Management Lifecycle

1. INCIDENT NAME:	**2. OPERATIONAL PERIOD**		**CRITICAL INFORMATION REQUIREMENTS**						
	FROM:	TO:							
3. CRITICAL INFORMATION REQUIREMENT (CIR)	**4. Requested By**	**5. Collected By**	**6. Reporting Timeline**				**7. Dissementaion Method**		
			Immediate Reporting	C&GS MTG	Planning MTG	Other (Specify)	Brief	209	Display
General Safety of Personnel, Near Misses	All UC	SOFR		X	X		X	X	
Safety of Personnel; Death or Significant Injury of Responder	All UC	All	X	X	X	Daily SITREP @ 0600	X	X	
Safety of Personnel; Anytime OPS halted by SOFR	All UC	SOFR	X	X	X	Daily SITREP @ 0600	X	X	
Accountability of Personnel/Status	All UC	RESL				Daily SITREP @ 0600		X	
Accountability of Resources/Status	All UC	RESL				Daily SITREP @ 0600		X	
Equipment Casualty/CASREP	All UC	OSC/RESL	X	X	X		X	X	
Environmental Resources at Risk	All UC	ENVL/SITL		X	X	Daily SITREP @ 0600	X	X	X
Environmental Resources at Risk; First impact of oil to wildlife	All UC	ENVL/SITL	X				X		
Environmental Resources at Risk; First impact of oil to land	All UC	ENVL/SITL	X				X		
Economic Resources at Risk	All UC	SITL		X	X	Daily SITREP @ 0600	X	X	X
Economic Resources at Risk; Impacts to Marine Transportation System	USCG IC	MTSL		X	X	Daily SITREP @ 0600	X	X	X
Stakeholder Interest/Concerns	All UC	LOFR		X	X		X		
Stakeholder Interest/Concerns: Political Implications	All UC	LOFR	X				X		
Media Interest/Concerns	All UC	PIO		X	X		X		
Media Interest/Concerns: Adverse Media Coverage	All UC	PIO	X				X		
Major Shift in Planned Operations	All UC	OSC	X				X		

Appendix B
Best Practices When Using the Homeland Security Information Network (HSIN)

Introduction:

The Homeland Security Information Network (HSIN) is a vital tool for sharing information. The platform is nationally trusted and secure for federal, state, local, private, and international partner use. The program provides virtual meeting space, instant messaging, and document sharing in real-time. HSIN consists of an array of secure Communities of Interest (COIs) for users to collaborate. The COIs are divided into state organizations, federal organizations and distinct mission areas, to include emergency management, law enforcement, critical sectors, and intelligence. As a best practice, the area plans (i.e. ACP, AMSP, etc.) can pre-identify representative persons in need of HSIN account access and DHS employees can sponsor private sector representatives as a pre-planning process.

If a COI in HSIN is not available for use due to access and permissions, Adobe Connect may be of benefit. The use of HSIN or Adobe Connect during a response can be of vital importance, and may greatly impact the timeliness of sharing information.

Purpose:

The purpose of this plan is to provide a framework for information sharing during a response that meets timeliness and security concerns and needs. The platform provides multiple tools to support seamless collaboration. In order to facilitate collaboration during a large response, a host can set up multiple Adobe Connect Meetings for use and collaboration during a response (ex. Command Staff Meeting, Planning Section Meeting, IC/UC Meeting, and a meeting for Common Operation Picture).

Mandatory Criteria:

- All members of the Unified Command must agree to the use of HSIN.
- At least one representative from each agency in the Unified Command must be granted access.
- All persons must agree to the use of the Homeland Security Information Network (HSIN) Plan, and a form must be signed in person at the HSIN Connect Coordinator's Desk prior to electronic entry into the Meeting Room.

Directions to enter HSIN Connect:

- Once you have read the Use of the Homeland Security Information Network (HSIN) Plan and have signed the User Agreement at the check-in desk, the check-in personnel will provide you a link to enter the HSIN Adobe connect sites.
- Type in the provided link.

- If you do not already have a HSIN account, notify LT Overcash and you will be added you to the meeting. If you do not have an account, request to enter as a guest. When you enter as a guest, you must include your title and full name, including middle initial and agency (ex. LT Joe J. Smith (USCG)).
- A Site Host will approve your access into the site.
- Contact the Site Host if you have any questions.

Best Practices for Successful HSIN Connect use:

- All users and guests must sign the Use of the Homeland Security Information Network (HSIN) Plan User Agreement.
- Only personnel with Host Privileges can accept guests into the room.
- When a Meeting is initiated, ensure "Only registered users and accepted guests may enter the room."
- If a user accidently allows all guests with a link direct access to the site without initial verification, then the meeting must be ended, the access reset to "Only registered users and accepted guests" and then restarted. As a result, all guests will have to log back in and request guest access using the previously provided link.
- If a live feed of program (i.e. AIS, ERMA, etc.) is needed, the Host of the site can share their desktop in the Common Operational Picture meeting.
- The first pod created should be in the upper left hand corner and state the "Rules of the Road" for the room. Example below:

Guests: Please enter your name and agency affiliation when signing in as a guest.
If necessary your privileges will be upgraded by a HOST.

ONLY HOSTS CAN ACCEPT PERSONS INTO A MEETING ROOM

The Unified Command has directed that HSIN be used for interagency documentation and collaboration.

All response information (IAPs, SITREPS, 220s, etc..) be accessed by CG Agency Reps (as assigned by the Liaison Officer and approved by the IC) on the Exercise HSIN site.

ICP members will not support CG individual requests for information from the Exercise HSIN sites unless directly involved in the Exercise or District Senior Leadership support.

- If an Adobe Connect Meeting is being used as COP and the IAP complication site, the following is naming convention is required for the IAP compilation portion of the site.
    - Submit labeled "DRAFT IAP DOCUMENTS." All documents uploaded to this pod must have a DRAFT watermark, be digitally signed by the author, and saved with the following naming convention (DDMMMYY_FORM_AUTHOR → 15APR25_202_Johnson)
    - The Planning Section Chief creates a pod named "FINAL DOCUMENTS." All documents uploaded to this pod must be in .pdf format, digitally signed by the

Planning Section Chief, and saved with the following naming convention (DDMMMYY_DOCNAME_FINAL → 15APR25_IAP5_FINAL)

- Dedicate one pod to response pictures. All pictures uploaded must be labeled with the following naming convention:

  LAST NAME_SECTION_LOCATION_DATE_LETTER
  SMITH_OPS_XXX_07092025_A
  SMITH_OPS_XXX_07092025_B

  a. Photographer's last name
  b. ICS section assigned
  c. Geographic location photo was taken (e.g. segment or waterway)
  d. Date photo was taken. Year, month, day (e.g. 20250309 = March 9, 2025)
  e. Multiple photos from the same date and location will be differentiated with an alpha designator. (e.g. photo 1=A, photo 2=B, » » photo 27=AA)