



Analyst's Desktop Binder

Department of Homeland Security
National Operations Center
Media Monitoring Capability
Desktop Reference Binder

August
2013

Contents

1. Media Monitoring Capability Mission & Reporting Parameters..... 7

 1.1 MMC Mission..... 7

 1.2 Leverage Operationally Relevant Information..... 7

 1.3 Identify Relevant Operational Media..... 7

 1.4 Increase Situational Awareness of the DHS Secretary 8

2 Department of Homeland Security (DHS) Component Agencies 8

3 DHS National Operations Center (NOC) Phases of Reporting..... 10

 3.1 NOC Notes..... 10

 3.2 Monitored..... 10

 3.3 Awareness..... 10

 3.4 Phase 1 – Guarded 10

 3.5 Phase 2 – Concern..... 10

 3.6 Phase 3 – Urgent..... 11

 3.7 Events of High Media Interest or International Significance..... 11

 3.8 NOC Numbered Items 11

4 Items of Interest (IOI): 12

 4.1 Incidents that warrant an IOI: 12

 4.2 NOC Comprehensive Critical Information Requirements (CIR) & Essential Elements of Information (excerpt applicable to MMC):..... 13

 4.2.1 CIR #1 – Facts, Estimates & Projections about the Threat, Incident, Event or Storm: 13

 4.2.2 CIR #2 – DHS Readiness & Preparedness:..... 15

 4.2.3 CIR #3 – Other Federal, State, Local Readiness & Mitigation Actions: 15

 4.2.4 CIR #5 – Life Saving & Critical Resources / Shortages:..... 16

 4.2.5 CIR #6 – Damage & Restoration: 16

 4.2.6 CIR #7 – People:..... 17

 4.2.7 CIR #8 – Health & Safety:..... 17

 4.2.8 CIR #9 – Response and Recovery Organization & Leadership:..... 17

 4.2.9 CIR #10 – Long Term Recovery and Economic Impacts: 17

 4.2.10 CIR #11 – Public Information Guidance 18

 4.2.11 CIR #12 – Weather and Seas 18

 4.3 Key Words & Search Terms 18

4.4	Adding Search Terms & Sites:.....	21
4.5	Adding Twitter Accounts to “Follow”	22
4.6	IOI Categorization:	22
4.7	IOI Relevancy Rating Scale.....	23
4.8	Sourcing Items of Interest.....	24
4.8.1	Traditional Media.....	24
4.8.2	Social Media	24
4.9	Credible Sources for Corroboration.....	25
4.10	IOI Distribution Lists:.....	26
4.11	Creating IOIs (Traditional Media Application)	26
4.12	Creating IOIs (Social Media Application).....	28
4.13	Application – IOI (Uploading Images):.....	29
4.14	Outlook – IOI Backup (Traditional Media):	33
4.15	Outlook – IOI (Social Media):	34
4.16	IOI Corrections:	35
5	The Common Operational Picture (COP 3.1).....	36
5.1	MMC COP Operations	37
6	Personally Identifiable Information (PII):.....	40
6.1	Privacy Impact Assessment	41
6.2	Quality Control	41
6.3	Inadvertent PII (Redaction).....	41
7	Operational Summary (OPSUM):.....	42
7.1	Operational Summary (OPSUM) Format:	42
8	NOC Priorities:	45
8.1	NOC Priorities (HSIN Retrieval).....	46
9	Technology Suite	50
9.1	Audio Video System:.....	51
9.1.1	Direct TV Full Channel List	52
9.1.2	Direct TV Account Information.....	52
9.2	Online Audio-Video Switch.....	52
9.3	Mapping Shared Network Drive	53

10 HSIN (b) (7)(E) Connection Instructions: 54

11 Usernames, Passwords & Contact Information: 56

 11.1 Passwords – See Internal Password Sheet 56

 11.2 NOC Contact Information..... 57

 11.2.1 The SWO/KMO: 57

 11.2.2 HSIN Help Desk: 57

 11.2.3 TSI Senior Reviewers: 57

12 Responsible Official..... 58

--	--	--	--

1. Media Monitoring Capability Mission & Reporting Parameters:

1.1 MMC Mission

The MMC has three primary missions:

- Continually update existing National Situation Summaries (NSS) and International Situation Summaries (ISS) with the most recent, relevant, and actionable open source media information.
- Dynamically monitor available open source information with the goal of expeditiously alerting the NOC Watch Team and other key Department personnel of emergent incident management situations such as terrorist activities, natural or man-made disasters and public safety.
- Receive, process, and distribute media captured from streaming sources available to the NOC such as Northern Command's (NORTHCOM) Full Motion Video (FMV) and via open sources.

These three missions are accomplished with strict adherence to the approved NOC MMC PIA of Jan 6, 2011 by employing various tools, services, and procedures that are described in detail in this document. The primary missions have three key components:

1.2 Leverage Operationally Relevant Information

Leveraging news stories, media reports, and postings on social media sites available to the public, concerning Homeland Security, Emergency Management, and National Health for operationally relevant data, information, analysis, and imagery is the first mission component. The traditional and social media teams review a story or posting from different perspectives and interests, utilizing thousands of reporters, sources, still/video cameramen, analysts, bloggers, and ordinary individuals on scene. Traditional Media outlets provide insight into the depth and breadth of the issue, including worsening situations, federal preparations, response activities, and critical timelines. At the same time, Social Media outlets provide instant feedback and alert capabilities to rapidly changing or newly occurring situations. The MMC summarizes the extensive information from these resources to enrich the operational picture for the Department of Homeland Security, without including unauthorized Personally Identifiable Information (PII).

1.3 Identify Relevant Operational Media

Supporting the NOC by ensuring they have a timely awareness of evolving Homeland Security news stories and media reports of interest to the public and DHS/other federal agencies involved in preparations and response activities is the second key component. DHS and other federal agencies conducting joint operations may be affected by evolving situations in that area. These situations may not be directly related to an ongoing issue but may also have an indirect effect. Through coordination with the NOC Duty Director (NDD) or the Senior Watch Officer (SWO), the MMC works to ensure the NOC Watch Team is aware of such stories and news events and has time to analyze any effect on operations. In all cases, the MMC follows a protocol for ensuring source credibility and data accuracy. Authorized PII is included in the reports only to the extent that it lends credibility to the report.

Timely reporting of current information is an integral element in maintaining operational awareness by Homeland Security personnel. The MMC understands it is vital that critical information is relayed to key Department decision makers as expeditiously as possible.

1.4 Increase Situational Awareness of the DHS Secretary

Mitigating the likelihood that the Secretary and DHS executive staffs are unaware of a breaking Homeland Security news story or media report is the third component. The Secretary and executive staff members are subject to press questions regarding domestic and international events, and may or may not be informed of the most current media coverage. The MMC understands Critical Information Requirements and NOC Daily Priorities, and monitors news coverage with the perspective of how the breaking story may be related to current and other important ongoing situations and DHS activities. DHS Senior Leadership, the NOC, and the MMC are concerned with and report on what is being reported, not who is reporting it.

The on-duty MMC analysts alert DHS personnel and related federal agencies of updated news stories through distributed Items of Interest (IOI). MMC strives to identify and integrate media coverage to report situations of operational relevance that must be brought to the attention of the Secretary and/or senior leadership.

2 Department of Homeland Security (DHS) Component Agencies

The **Directorate for National Protection and Programs** works to advance the Department's risk-reduction mission. Reducing risk requires an integrated approach that encompasses both physical and virtual threats and their associated human elements.

The **Directorate for Science and Technology** is the primary research and development arm of the Department. It provides federal, state and local officials with the technology and capabilities to protect the homeland.

The **Directorate for Management** is responsible for Department budgets and appropriations, expenditure of funds, accounting and finance, procurement; human resources, information technology systems, facilities and equipment, and the identification and tracking of performance measurements.

The **Office of Policy** is the primary policy formulation and coordination component for the Department of Homeland Security. It provides a centralized, coordinated focus to the development of Department-wide, long-range planning to protect the United States.

The **Office of Health Affairs** coordinates all medical activities of the Department of Homeland Security to ensure appropriate preparation for and response to incidents having medical significance.

The **Office of Intelligence and Analysis** is responsible for using information and intelligence from multiple sources to identify and assess current and future threats to the United States.

The **Office of Operations Coordination and Planning** is responsible for monitoring the security of the United States on a daily basis and coordinating activities within the Department and with governors, Homeland Security Advisors, law enforcement partners, and critical infrastructure operators in all 50 states and more than 50 major urban areas nationwide.

The **Federal Law Enforcement Training Center** provides career-long training to law enforcement professionals to help them fulfill their responsibilities safely and proficiently.

The **Domestic Nuclear Detection Office** works to enhance the nuclear detection efforts of federal, state, territorial, tribal, local governments and the private sector and to ensure a coordinated response to such threats.

The **Transportation Security Administration (TSA)** protects the nation's transportation systems to ensure freedom of movement for people and commerce.

United States Customs and Border Protection (CBP) is one of the Department of Homeland Security's largest and most complex components, with a priority mission of keeping terrorists and their weapons out of the U.S. It also has a responsibility for securing and facilitating trade and travel while enforcing hundreds of U.S. regulations, including immigration and drug laws.

United States Citizenship and Immigration Services secures America's promise as a nation of immigrants by providing accurate and useful information to our customers, granting immigration and citizenship benefits, promoting an awareness and understanding of citizenship, and ensuring the integrity of our immigration system.

United States Immigration and Customs Enforcement (ICE) promotes homeland security and public safety through the criminal and civil enforcement of federal laws governing border control, customs, trade, and immigration.

The **United States Coast Guard** is one of the five armed forces of the United States and the only military organization within the Department of Homeland Security. The Coast Guard protects the maritime economy and the environment, defends our maritime borders, and saves those in peril.

The **Federal Emergency Management Agency (FEMA)** supports our citizens and first responders to ensure that as a nation we work together to build, sustain, and improve our capability to prepare for, protect against, respond to, recover from, and mitigate all hazards.

The **United States Secret Service (USSS)** safeguards the nation's financial infrastructure and payment systems to preserve the integrity of the economy, and protects national leaders, visiting heads of state and government, designated sites, and National Special Security Events.

3 DHS National Operations Center (NOC) Phases of Reporting

NOTE: The NOC SOP goes into more detail on NOC reporting and is available at each MMC desk.

3.1 NOC Notes

NOC Notes are produced by the NOC whenever there is a situation that could potentially require Federal assets such as personnel, equipment, or funding. In such cases, this would be an ongoing event, and a NOC-assigned number will be used for labeling and monitoring the situation (MMC will get notice via blast call, email, or pager). These IOIs have higher precedence over regular IOIs, but could either develop into an Awareness or become resolved rather quickly. These do not get added to the COP (only Monitored or higher reports), but the MMC will continue to publish IOIs on the event until the NOC determines that the situation has been resolved.

3.2 Monitored

The Monitored status is given to NOC reports which require NOC attention, but could be considered routine and do not rise to the level of an Awareness report. Suspicious activities, devices, packages, unsubstantiated bomb threats, and other incidents currently being assessed and addressed by federal, state, or local authorities will normally be tracked under the Monitored status.

3.3 Awareness

Awareness reports are those that have a higher precedence over general IOIs or NOC Notes (many Awareness reports are a result of a NOC Note), but the reporting requirement has not been increased to the point of Phase reports. Each of these covers a singular event that could be upgraded to a Phase item as the situation evolves or escalates. Awareness reports are generated for National and International events that may be of interest to DHS, and are usually handled at the local and State level. The incidents usually require only DHS situational awareness, monitoring, and routine reporting. NSSE or SEAR Level 1 or 2 events whose public safety nexus, threat, complexity, or other attributes require Federal information-sharing and Federal operations coordination and planning activities without a specific threat.

3.4 Phase 1 – Guarded

Phase 1 reports focus on manmade events, natural disasters, and other incidents that State and local officials will manage with the limited federal assistance of one or more DHS Components. Suspicious activities, events, incidents, or accidents that could become a matter of interest at the national level or events with a significant impact on Federal Tier 1 critical infrastructure would also fall under Phase 1 reporting. Phase 1 reporting would also be initiated for events that have a homeland security or public safety nexus that the National Security Staff, Secretary, and/or senior DHS officials may need to address.

3.5 Phase 2 – Concern

Phase 2 reports cover any event that meets one or more of the four criteria outlined in Homeland Security Presidential Directive – 5.

1. A federal department or agency acting under its own authority has requested the assistance of the Secretary.
2. The resources of state and local authorities are overwhelmed and federal assistance has been requested by the appropriate state and local authorities.

3. More than one federal department or agency has become substantially involved in responding to the incident.
4. The Secretary has been directed to assume responsibility for managing the domestic incident by the President.

Incidents that require Phase 2 reporting include manmade events and natural disasters causing loss of life or industrial accidents occurring in densely populated areas with potential public safety or public health impacts. Credible threats with a known time, location, and method as determined by the intelligence or law enforcement community characterized by possible/confirmed terror nexus with U.S. homeland security implications would also be reported under Phase 2. An event or incident requiring a coordinated Federal response in which two or more DHS Components are substantially involved would also fall under Phase 2 reporting.

3.6 Phase 3 – Urgent

Phase 3 reporting is characterized by an event so catastrophic that the Federal government must assume the highest level of operational posturing and activity.

3.7 Events of High Media Interest or International Significance

Periodically, there are events that the NOC constantly monitors – both national and international – and are listed on the NOC Priorities and Monitoring Report. The MMC will monitor such events to see if an IOI is warranted. Usually these events will be included in the OPSUM even though they may not have a NOC number assigned, and in this case, would simply be used to enhance situational awareness. Some of these events may be issued a NOC-assigned number and in this case, the MMC will publish IOIs in the same manner as it would for NOC Notes, Awareness, or Phase reports. These do not get added to the COP unless the NOC directs the MMC to do so.

3.8 NOC Numbered Items

On occasion, the NDD/SWO will determine that an incident is worth tracking; however, it may not be substantial enough to warrant the generation of a higher level report, such as a NOC Note, Awareness, or Phase report.

NOC Numbers may be utilized for any type of incident and usually follow the [NOC #0000-00: Incident Title] format. However, if an incident falls under the Public Safety or Suspicious Activity category, the NOC may issue an item in the [NOC #0000-00-000: Incident Title] format. In those cases, incidents will be issued one of the following NOC Numbers, with the addition of a 3-digit tracking number at the end:

- **NOC #0012-12: Suspicious Activity – Chemical, Biological, Radiological, Nuclear or Explosive (CBRNE):** Covers any suspicious incident which may involve a CBRNE or CBRNE threat
- **NOC #0013-12: Suspicious Activity:** Covers any suspicious incident which does not involve a CBRNE
- **NOC #0014-12: Public Safety/Unusual Activity:** Covers any incident that is not suspicious in nature, but needs further information or tracking

Example: NOC 0012-12-295 [Suspicious Powder, Anchorage, AK]

If included on the NOC Priorities list for the day, these incidents will be summarized in the OPSUM.

If the NOC issues a close-out for a numbered incident, but the MMC continues to find significant reportable information, analysts will continue to use the assigned NOC # for additional distributions.

4 Items of Interest (IOI):

MMC coverage focuses primarily on providing information on incidents, significant events and crises, which are usually defined as catastrophic events that result in wide-scale damage or disruption to the nation's critical infrastructure, key assets, or the nation's health; and require a coordinated and effective response by Federal, State, and Local entities. For the most part, coverage of international incidents is limited to that of terrorist activities and infectious diseases that impact a wide population of humans or animal stock, such as mad cow disease or H5N1, and catastrophic weather events around the globe (Category 5 Hurricanes, Tsunami, and Large Magnitude Earthquakes). An Item of Interest (IOI) is generated whenever an MMC search or alert produces information about an emergent incident that should be brought to the attention of the NOC. The emphasis in IOI reporting is always focused on operationally relevant information, the "what" versus the "who." In preparing and distributing IOIs, analysts must only include authorized PII. Further, analysts must consider whether inclusion of authorized PII lends credibility to the report before distributing an IOI containing authorized PII. Often PII may be found in the text of the reports when referring to specific individuals or in the text of the source links (e.g., <https://twitter.com/#!/sallyreporter>).

Note - If there are ANY questions about whether an incident or other reported item is IOI-worthy, check with MMC leadership.

4.1 Incidents that warrant an IOI:

- Terrorist incidents (including foreign countries)
- Major natural disasters (e.g., floods, tornadoes, earthquakes)
- Transportation incidents where major bottlenecks may occur or where chemical/explosive hazards exist
- Incidents that could result in injury to a local population (e.g., fire at a chemical production facility releasing toxic fumes)
- Incidents that result in damage to critical infrastructure
- Safety issues (e.g., aircraft emergency)
- Certain crimes (e.g., snipers, mall/school shootings, major drug busts, illegal immigrant busts, etc)
- Policy directives and implementations operationally related to DHS

Note - Analysts are to refrain from generating IOI reports that:

- 1) *Include any form of unauthorized PII*
- 2) *Include public reaction to DHS programs, policies and procedures unless they are operationally relevant (e.g., long wait times at TSA checkpoints)*

- 3) Focus on individuals' First Amendment-protected activities unless they are operationally relevant (e.g., protest shuts down I-95 – in which case, the report should focus on impact to operations and not the subject of the protest)
- 4) *Overview proposed legislation or legal challenges on enacted legislation*
- 5) *Have an obvious political bias or agenda*
- 6) *Are predictive or futuristic*

4.2 NOC Comprehensive Critical Information Requirements (CIR) & Essential Elements of Information (excerpt applicable to MMC):

4.2.1 CIR #1 – Facts, Estimates & Projections about the Threat, Incident, Event or Storm:

a. Chemical or Biological Attacks

What Information is known about the chemical or biological agent of concern and what are typical symptoms indicating exposure?

What are the safe and dangerous exposure levels, related medical procedures and/or antidotes?

What are the known distances from the location of release from major population centers?

What do the plume modeling and forecasts indicate?

Is there information on documented water and food contamination?

b. Cyber Attacks

What are the critical facts about the extent of the cyber attack?

Were any key national programs or data systems targeted, exposed or impacted? If exposed or impacted, what is the known extent of the damage or compromise of data?

Is there an estimated source of attack and other relevant information regarding the cyber attack?

c. Earthquakes

Where exactly was the epicenter of the earthquake located and provide details in relation to the distances from major metropolitan center(s) or landmark(s).?

What were the Richter scale measures of the earthquake?

How far apart in distances throughout the region was the earthquake felt or impacted?

What is the estimated population most affected by the earthquake?

What are the anticipated aftershocks and for what period / duration will they last?

d. Explosions

What are the critical facts about the explosion (i.e. source(s) or agent(s) or explosive materials used)?

What were the measures or estimates of the explosion's force?

What was the location of impact to buildings?

Are any Critical Infrastructure or Key Resources affected?

e. Fires

Where is the fire located?

What is the distance from the fire to populated areas (i.e. residential, business, etc)?

What is the size of the fire?

What percentage is contained?

Are there any forecasted and/or factual issues for consideration?

Do fire officials suspect a cause of the fire?

Has a Fire Management Assistance Grant (FMAG) been requested and/or approved?

f. Floods

What are the projected or estimated flood levels? River levels? Estimated peaks?

What are the cities and population centers impacted (or will be impacted)?

g. Hurricanes

What Hurricane category applies to this storm?

What are the maximum and sustained winds?

What and where is the anticipated storm surge and flooding risk?

What is the storm diameter, location of eye, barometric pressures, and projected track?

When is the anticipated landfall date/time and where is the storm projected to arrive at?

h. Oil Spill of National Significance or Hazardous Material Spill

What are the critical facts about the oil or hazardous material spill (i.e. estimates on size and rate of spill, current location, and sources(s) and date/time of spill)?

What do computer projections or modeling indicate with respect to spill drift speed and direction?

What are considered to be safe and dangerous exposure levels (if applicable)?

Has a responsible party for the spill been identified? (*MMC must never include PII*)

Are there any sensitive environmental areas (i.e. Wildlife Preserve, Conservation Areas, Habitats, etc) that could be adversely impacted by the spill?

What other relevant information about the spill must be considered?

i. Mass Migration

What are the estimates of total migrants attempting to migrate?

What are the likely countries of origin and U.S. destinations?

How many migrants have been intercepted or rescued to date?

Are there any fatalities or serious injuries?

j. Nuclear and Radiological Attack, Incident, or Release

What is the source of the release?

What are the current radiation levels at the various rings / distances from the release location and from major population centers?

What do plume modeling forecasts indicate for radiation contamination?

Have any safe and dangerous exposure levels been identified?

Is there information on documented water and food contamination? What agencies are responsible and in charge of monitoring this threat?

k. Pandemic Influenza or Outbreak

What is the critical information regarding the nature of the pandemic or influenza outbreak?

Have incubation periods been identified?

What are the associated symptoms with this outbreak?

Are there any special concerns for elderly persons or infants?

Are there any prescribed medical treatments or shots identified and/or available?

l. Special Events

What are the critical facts and information about the event (i.e. security, location, facilities, etc)?

m. Suspicious Activity or Suspicious Package

What are the critical facts about the suspicious activity or package, including a description of the activity or package, the location and nearness to major population centers or landmarks and the proximity to critical infrastructure or facilities?

List other pertinent details on what local law enforcement authorities have been notified (if any); or details on what explosive ordinance responders have been notified (if any).

n. Terrorism Threat

What are the specific details of the credible threat (methods and means for carrying out the threat, etc)?

o. Tornadoes and Other Severe Weather

What are the critical facts and description of the tornadoes or storm (to include maximum and sustained winds, storm diameter, location, and barometric pressures)?

What is the projected track of the storm?

What is the anticipated landfall date/time and arrival location?

p. Tsunamis

What are the estimated wave heights, location, and duration of the tsunami?

What is the estimated date/time to arrive at Continental U.S. (CONUS) shores or major population centers?

What is the estimated speed and direction of the tsunami?

Is there a discrepancy between observed versus forecasted data?

4.2.2 CIR #2 – DHS Readiness & Preparedness:

a. National Terrorism Advisory System (NTAS)

What are the pertinent details of any threat that drives an NTAS alert (i.e. type of threat, source, timeline, potential impact to public, etc)?

What are the recommended preventive measures to take in order to heighten public safety (by communities, businesses, and government entities) e.g. lockdowns, evacuations, etc.?

b. DHS Protective Measures and Actions

What are the DHS protective measures or mitigation steps being exercised or planned to limit the impact to DHS mission readiness and response operations?

What offices, teams or task forces were impacted or affected by this threat, event or incident, if any?

What is the status of DHS's specialized teams needed to respond to this threat, incident or storm?

What are the DHS protective measures or mitigation plans or actions being exercised or planned for responding to this terrorist threat? (Note, this info is important for CIKR facilities or transportation infrastructure especially).

What are the estimated effects these protective measures or mitigation plans have on national supply system, key transportation nodes or commerce, if any?

Are there any advisories or public warnings being issued?

4.2.3 CIR #3 – Other Federal, State, Local Readiness & Mitigation Actions:

a. Evacuation Plans and Estimates

What is the general evacuation plan for this event or incident?

- What is the estimated number of general population requiring evacuation?
- Have federal, state, tribal, territorial, and/or local authorities identified any areas for evacuation (mandatory or voluntary)?

What is the status of evacuation orders, if any?

Have there been any problems with personnel evacuation or applicable evacuation plans?

What is the rough re-entry plan for the evacuated general public to return?

Will there be any quarantine required or anticipated for the public prior to re-entry? If so, what are the essential details?

b. Changes to Security Levels or U.S. Conditions of Readiness

Has this threat, incident or event resulted in changes to any U.S. condition of readiness, such as Department of Defense Condition (DEFCON), Force Protection Condition (FPCON), Information Operations Condition (INFOCON) or USCG Maritime Security (MARSEC) Levels?

4.2.4 CIR #5 – Life Saving & Critical Resources / Shortages:

a. Status of First Responders

How has this event or incident affected the first responders' (fire, police, medical) ability to provide needed support to the affected communities?

Is there a Mutual Aid agreement already in place among regional fire, police, and emergency medical services? If so, what are the pertinent details?

What is the re-entry plan for first responders?

What is the status of medical response personnel?

Is there an anticipated need for search and rescue operations as a result of this event or incident? If so, what DHS agencies and assets will be providing support or likely be used?

What is their status?

What Department of Defense assets are likely to be used? What is their status?

What National Guard assets are likely to be used? What is their status?

b. Life Saving & Other Critical Response / Recovery Actions

What are the major or critical requests for assistance that DHS is responsible for or responding to?

- o Who made the request(s) and what are the relevant dates/deadlines of the request (e.g. Foreign State, Department of State, state, local government, etc)?

What are the major DHS assets or teams requested or already responding to this incident (i.e. IMATs, Vessels, Teams, etc)?

What major operational response actions are being taken in response to the threat, event or incident?

c. Status of Food, Water, Shelter, Power, and Communications

What is the status of food, water, shelter, power and communications in the affected region?

d. Critical Resource Gaps, Unmet Needs, and Medical Shortfalls

Has any Federal, State or Local government or responding agency identified any critical resource gaps or major operational response or asset gaps that cannot be resolved?

e. Status of Coast Guard Reserve Personnel

Has the President authorized the recalling of Title 10 forces to provide support as a result of this event or incident?

Has the U.S Coast Guard activated their Coast Guard Reserve workforce? What are the associated details?

4.2.5 CIR #6 – Damage & Restoration:

a. CIKR (Level One) Damage Estimates and Restoration Actions

What major Critical Infrastructure and Key Resources (CIKRs) will likely be impacted or have been impacted as a result of this event or incident?

Which impacted CIKRs are the most critical to recovery operations?

What is the projected damage or impact to these CIKRs as a result of this event or incident?

- What are the likely cascading effects that will ensue as a result of the damage to these listed CIKRs?
- What is the long term (greater than 6 months) regional, state and national impact as a result of the damage to these listed CIKRs?

What are the major DHS restoration activities being executed to help restore CIKR facilities and infrastructure?

b. Other CIKR Damage Estimates

What other Critical Infrastructure and Key Resources (CIKRs) will likely be impacted or have been impacted as a result of this event or incident?

What is the projected damage or impact to these CIKRs as a result of this event or incident?

What are the major DHS restoration activities being executed to help restore CIKR facilities and infrastructure?

4.2.6 CIR #7 – People:

Status of U.S. Public (in General)

What are the general estimates for number of U.S. citizens impacted or projected to be impacted by this threat, event or incident?

What is the estimated and confirmed number of deaths, injuries or missing persons as a result of this event or incident?

What is the estimated number of personnel and special needs personnel that might require rescuing as a result of this event or incident?

How many homes were destroyed or damaged as a result of this event or incident?

How many personnel are estimated and confirmed to be homeless as a result of this event or incident?

4.2.7 CIR #8 – Health & Safety:

a. Major Health Concerns and Estimates

What are the general estimates for number of U.S. citizens impacted (or will be impacted) by this health-related event or incident?

What are the anticipated effects to U.S. health as a result of this event or incident?

What are the current estimates or confirmed cases of individuals with communicable disease, pandemic like symptoms or confirmed diagnosis?

What are the worst case estimates for communicable disease and/or pandemic outbreak as a result of this event or incident?

b. Quarantine & Similar Health and Safety Plans

Are there any plans by the Federal, State, or Local government to implement quarantine plans in response to an incident or threat?

4.2.8 CIR #9 – Response and Recovery Organization & Leadership:

Lead Agency, Response and Recovery Organization(s)

Who is the lead Federal, State, and Local agency responsible for responding to this threat, incident, event or storm?

What is the primary State or Local Emergency Operation Center (or similar command) established to coordinate all the state and local response actions to this incident?

4.2.9 CIR #10 – Long Term Recovery and Economic Impacts:

a. Estimates on Long Term Recovery Operations

What are the damage estimates as a result of the impact from this event or incident? (Note: please provide specific emphasis on damage estimates to the communications, energy, and transportation sectors.)

What are the major long term effects (greater than 6 months in duration) as a result of this event or incident?

What is the estimated recovery time from this event, incident or storm?

b. Economic & Other Strategic National & Long Term Consequences

What is the estimated strategic U.S. National impact resulting from this event or incident?

- o What is the anticipated impact on the U.S. economy?

What is the anticipated impact on the U.S. environment? What are the estimated long term consequences to the geographic region affected by this incident or event?

4.2.10 CIR #11 – Public Information Guidance

What additional information regarding this incident and DHS’s role in it can be found amongst popular social networks, press releases, and public statements?

4.2.11 CIR #12 – Weather and Seas

What is the forecasted weather and seas (e.g. next 72 hours) for the area(s) or region(s) in question or in the area(s) where DHS operations are ongoing?

Any other relevant high-level weather related information?

4.3 Key Words & Search Terms

This is a current list of terms that will be used by the NOC when monitoring social media sites to provide situational awareness and establish a common operating picture. As natural or manmade disasters occur, new search terms may be added. Any new search term added that is not from this list must be approved by the shift lead and emailed to the MMC PM. The new search terms will not use PII in searching for relevant mission-related information

DHS & Other Agencies

Department of Homeland Security (DHS)	Immigration Customs Enforcement (ICE)	U.S. Citizenship and Immigration Services (CIS)
Federal Emergency Management Agency (FEMA)	Agent	Federal Air Marshal Service (FAMS)
Coast Guard (USCG)	Task Force	Transportation Security Administration (TSA)
Customs and Border Protection (CBP)	Fusion Center	Air Marshal
Border Patrol	Drug Enforcement Administration (DEA)	Federal Aviation Administration (FAA)
Secret Service (USSS)	Secure Border Initiative (SBI)	National Guard
National Operations Center (NOC)	Federal Bureau of Investigation (FBI)	Red Cross
Homeland Defense	Alcohol, Tobacco, Firearms and Explosives (ATF)	United Nations (UN)

Domestic Security

Assassination	Law enforcement	National preparedness
Attack	Authorities	Mitigation
Domestic security	Disaster assistance	Prevention
Drill	Disaster management	Response
Exercise	DNDO (Domestic Nuclear Detection Office)	Recovery
Cops		Dirty bomb

Domestic nuclear detection
 Emergency management
 Emergency response
 First responder
 Homeland security
 Maritime domain awareness (MDA)
 National preparedness initiative
 Militia
 Shooting
 Shots fired
 Evacuation

Deaths
 Hostage
 Explosion (explosive)
 Police
 Disaster medical assistance team (DMAT)
 Organized crime
 Gangs
 National security
 State of emergency
 Security
 Breach
 Threat

Standoff
 SWAT
 Screening
 Lockdown
 Bomb (squad or threat)
 Crash
 Looting
 Riot
 Emergency Landing
 Pipe bomb
 Incident
 Facility

HAZMAT & Nuclear

Hazmat
 Nuclear
 Chemical spill
 Suspicious package/device
 Toxic
 National laboratory
 Nuclear facility
 Nuclear threat
 Cloud
 Plume
 Radiation
 Radioactive

Leak
 Biological infection (or event)
 Chemical
 Chemical burn
 Biological
 Epidemic
 Hazardous
 Hazardous material incident
 Industrial spill
 Infection
 Powder (white)

Gas
 Spillover
 Anthrax
 Blister agent
 Chemical agent
 Exposure
 Burn
 Nerve agent
 Ricin
 Sarin
 North Korea

Health Concern + H1N1

Outbreak
 Contamination
 Exposure
 Virus
 Evacuation
 Bacteria
 Recall
 Ebola
 Food Poisoning
 Foot and Mouth (FMD)
 H5N1
 Avian
 Flu
 Salmonella
 Small Pox
 Plague
 Human to human

Human to Animal
 Influenza
 Center for Disease Control (CDC)
 Drug Administration (FDA)
 Public Health
 Toxic
 Agro Terror
 Tuberculosis (TB)
 Agriculture
 Listeria
 Symptoms
 Mutation
 Resistant
 Antiviral
 Wave
 Pandemic

Infection
 Water/air borne
 Sick
 Swine
 Pork
 Strain
 Quarantine
 H1N1
 Vaccine
 Tamiflu
 Norvo Virus
 Epidemic
 World Health Organization (WHO) (and components)
 Viral Hemorrhagic Fever
 E. Coli

Infrastructure Security

Infrastructure security
Airport
CIKR (Critical Infrastructure
& Key Resources)
AMTRAK
Collapse
Computer infrastructure
Communications
infrastructure
Telecommunications
Critical infrastructure
National infrastructure
Metro
WMATA

Airplane (and derivatives)
Chemical fire
Subway
BART
MARTA
Port Authority
NBIC (National
Biosurveillance Integration
Center)
Transportation security
Grid
Power
Smart
Body scanner

Electric
Failure or outage
Black out
Brown out
Port
Dock
Bridge
Cancelled
Delays
Service disruption
Power lines

Southwest Border Violence

Drug cartel
Violence
Gang
Drug
Narcotics
Cocaine
Marijuana
Heroin
Border
Mexico
Cartel
Southwest
Juarez
Sinaloa
Tijuana
Torreón
Yuma
Tucson
Decapitated
U.S. Consulate
Consular
El Paso

Fort Hancock
San Diego
Ciudad Juarez
Nogales
Sonora
Colombia
Mara salvatrucha
MS13 or MS-13
Drug war
Mexican army
Methamphetamine
Cartel de Golfo
Gulf Cartel
La Familia
Reynosa
Nuevo Leon
Narcos
Narco banners (Spanish
equivalents)
Los Zetas
Shootout
Execution

Gunfight
Trafficking
Kidnap
Calderon
Reyosa
Bust
Tamaulipas
Meth Lab
Drug trade
Illegal immigrants
Smuggling (smugglers)
Matamoros
Michoacana
Guzman
Arellano-Felix
Beltran-Leyva
Barrio Azteca
Artistic Assassins
Mexicles
New Federation

Terrorism

Terrorism
Al Qaeda (all spellings)
Terror
Attack
Iraq
Afghanistan
Iran
Pakistan
Agro

Environmental terrorist
Eco terrorism
Conventional weapon
Target
Weapons grade
Dirty bomb
Enriched
Nuclear
Chemical weapon

Biological weapon
Ammonium nitrate
Improvised explosive device
IED (Improvised Explosive
Device)
Abu Sayyaf
Hamas
FARC (Armed Revolutionary
Forces Colombia)

IRA (Irish Republican Army)	Weapons cache	Extremism
ETA (Euskadi ta Askatasuna)	Suicide bomber	Somalia
Basque Separatists	Suicide attack	Nigeria
Hezbollah	Suspicious substance	Radicals
Tamil Tigers	AQAP (AL Qaeda Arabian Peninsula)	Al-Shabaab
PLF (Palestine Liberation Front)	AQIM (Al Qaeda in the Islamic Maghreb)	Home grown
PLO (Palestine Liberation Organization)	TTP (Tehrik-i-Taliban Pakistan)	Plot
Car bomb	Yemen	Nationalist
Jihad	Pirates	Recruitment
Taliban		Fundamentalism
		Islamist
Weather/Disaster/Emergency		
Emergency	Ice	Mud slide or Mudslide
Hurricane	Stranded/Stuck	Erosion
Tornado	Help	Power outage
Twister	Hail	Brown out
Tsunami	Wildfire	Warning
Earthquake	Tsunami Warning Center	Watch
Tremor	Magnitude	Lightening
Flood	Avalanche	Aid
Storm	Typhoon	Relief
Crest	Shelter-in-place	Closure
Temblor	Disaster	Interstate
Extreme weather	Snow	Burst
Forest fire	Blizzard	Emergency Broadcast System
Brush fire	Sleet	
Cyber Security		
Cyber security	Keylogger	Brute forcing
Botnet	Cyber Command	Mysql injection
DDOS (dedicated denial of service)	2600	Cyber attack
Denial of service	Spammer	Cyber terror
Malware	Phishing	Hacker
Virus	Rootkit	Conficker
Trojan	Phreaking	Worm
	Cain and abel	Scammers

4.4 Adding Search Terms & Sites:

All of the tools utilized by the Traditional and Social Media teams are highly effective resources for locating salient information on breaking or evolving situations of interests to the DHS NOC. While these tools are all established in a standardized manner, it becomes necessary as situations develop, to add, edit, or adjust the search and source parameters that are used. When necessary, the protocol below will be followed for adding search terms or sources to MMC tools:

1. The Watch analyst will identify the source or keyword that he/she would like to utilize within MMC tools or general internet browser searches and submit it to the Watch Lead (Senior Analyst on shift).
2. The Watch Lead will approve or disapprove of the keyword term or source. If the Watch Lead believes that the source or keyword will add value or provide greater granularity to established searches, the item will be added to MMC tools/searches.
3. A note regarding the addition of a new keyword or source will be entered into the MMC's Daily Log, and a message identifying the change will be sent to MMC management. The new keyword term or source will also be provided to oncoming analysts during the next shift changeover brief.

4.5 Adding Twitter Accounts to "Follow"

Under no circumstances will MMC analysts "follow" the Twitter profiles of private citizens. However, in the course of conducting NOC/MMC business, MMC analysts may determine that a new Twitter profile needs to be added to the approved list of accounts that are followed. When additions are necessary, analysts will adhere to the process below for "following" an account:

1. The on-shift analysts agree that a Twitter profile should be added to the Twitter Profiles Followed list due to changing circumstances and NOC requirements.
2. The MMC Watch Lead approves the request and sends an email or (b) (7)(A), (b) (7)(C) request to the on-duty NOC SWO/ASWO for approval.
3. The NOC SWO/ASWO approves the request in an email or (b) (7)(A), (b) (7)(E) response back to the MMC analysts.

4.6 IOI Categorization:

The categorization of IOIs in the daily log allows analysts to track the types of articles that are distributed as they relate to 13 characterizations. The emphasis in IOI reporting is always focused on operationally relevant information, the "what" versus the "who." In preparing and distributing IOIs, analysts take great care to never include unauthorized PII anywhere in the report, including within the text of the source link. The characterizations include:

- 1) **Terrorism:** Includes media reports on the activities of terrorist organizations both in the United States as well as abroad. This category will also cover media articles that report on the threats, media releases by al Qaeda and other organizations, killing, capture, and identification of terror leaders and/or cells. Reports in this category CANNOT include the name of the terrorist unless deceased.
- 2) **Weather/Natural Disasters/Emergency Management:** Includes media reports on emergency and disaster management related issues. Reports include hurricanes, tornadoes, flooding, earthquakes, winter weather, etc. (all hazards). Reports will outline the tracking of weather systems, response and recovery operations, as well as the damage, costs, and effects associated with emergencies and disasters by area. Will also include articles regarding requests for resources, disaster proclamations, and requests for assistance at the local, state, and federal levels.

- 3) **Fire:** Includes reports on the ignition, spread, response, and containment of wildfires/industrial fires/explosions regardless of source.
- 4) **Trafficking/Border Control Issues:** Includes reports on the trafficking of narcotics, people, weapons, and goods into and out of the United States of an exceptional level. Reports will also include articles outlining the strategy changes by agencies involved in the interdiction of the items outlined above.
- 5) **Immigration:** Includes reports on the apprehension of illegal immigrants, policy changes having operational implications with regard to immigration in the United States, and border control issues. (Reports in this category CANNOT include the names of illegal immigrants.)
- 6) **HAZMAT:** Includes reports on the discharge of chemical, biological, and radiological hazardous materials as well as security and procedural incidents at nuclear facilities around the world and potential threats toward nuclear facilities in the United States. Also included under this category will be reports on, and responses to, suspicious powder incidents and chemical or biological agents.
- 7) **Nuclear:** Includes reports on international nuclear developments, attempts to obtain nuclear materials by terrorist organizations, and stateside occurrences such as melt downs, the mismanagement of nuclear weapons, releases of radioactive materials, illegal transport of nuclear materials, obtaining of weapons by terrorist organizations, and breaches in nuclear security protocol.
- 8) **Transportation Security:** Includes reports on security breaches, airport procedures, and other transportation-related issues. Reports will include threats toward and incidents involving rail, air, road, and water transit in the United States.
- 9) **Infrastructure:** Includes reports on national infrastructure, including key assets and technical structures. Reports will include articles related to failures or attacks on transportation networks, telecommunications/ internet networks, energy grids, utilities, finance, domestic food and agriculture, government facilities, and public health.
- 10) **National/International Security:** Includes reports on threats or actions taken against United States national interests both at home and abroad. Reports will include articles related to threats against American citizens, political figures, military installations, embassies, and consulates, as well as efforts taken by local, state, and federal agencies to secure the homeland. Articles involving intelligence will also be included in this category.
- 11) **Health Concerns, National/International:** Includes reports on national and international outbreaks of infectious diseases and recalls of food or other items deemed dangerous to the public health.
- 12) **Public Safety:** Includes reports on public safety incidents, building lockdowns, bomb threats, mass shootings, and building evacuations.
- 13) **Cyber Security:** Reports on cyber security matters that could have a national impact on other CIR Categories; internet trends affecting DHS missions such as cyber attacks, computer viruses; computer tools and techniques that could thwart local, state and federal law enforcement; use of IT and the internet for terrorism, crime or drug-trafficking; and Emergency Management use of social media

4.7 IOI Relevancy Rating Scale

The Item of Interest (IOI) Relevancy Rating Scale is a tool that provides MMC analysts with a process to assess the relevancy of a news story to DHS Operations and the urgency in which the corresponding IOI should be distributed. Determining the relevancy of an IOI allows analysts to triage news stories and send out time-sensitive pieces first, followed by less acute stories. The IOI Relevancy Rating Scale is broken down into five categories, from “Absolutely Send” to “Do Not Report.”

Rating	Threat Assessment	Distribution
5 - Absolutely Send	DHS OPS relevant/Breaking news - time sensitive	Immediate
4 – Send, not time sensitive	DHS OPS relevant, but not time sensitive	Not time sensitive
3 – Continue research and either rate as send or do not send	DHS relevance/Determine if worth distribution	Must determine if Category 4 or Category 2
2 – Marginal DHS Relevance	Marginal DHS relevance/Not in line with reporting guidance	Must be approved by MMC leadership for distribution
1 - Absolutely SHOULD NOT BE Reported	Not operationally relevant	None

4.8 Sourcing Items of Interest

Identifying the source of information allows the MMC to record the means by which articles are discovered. This does not involve recording PII of the specific content authors, but instead involves recording general source categories within either traditional or social media as noted below. Such metrics support MMC analysts/management in reviewing the productivity of certain tools/processes to assist in process improvement and quality assurance efforts. Characterization of sourcing includes:

4.8.1 Traditional Media

- 1) **Live Broadcast:** The Item of Interest was distributed following live television broadcast by FOX News, CNN, MSNBC, etc.
- 2) **Alert:** The Item of Interest was initiated because of an alert from the NOC.
- 3) **Passive Scan:** The Item of Interest was produced following the finding of an article as the analyst searched websites (Foxnews.com, CNN.com, BBC.co.uk, etc.) or through the use of the MMC’s aggregator tools.
- 4) **Active Search:** The Item of Interest was distributed after the analyst found an article by seeking out certain topics in search engines (Google, Yahoo, MSN, etc.)

4.8.2 Social Media

- 1) **Credible Source:** The item of interest was distributed following information provide by a credible source, such as a twitter posting by a media outlet
- 2) **Credible Evidence:** Information is provided by social media sources, but is being redistributed by other users or media outlets, lending credibility

- 3) **Corroborating “Hits” Indicating a Trend:** The item of interest was produced from multiple social media different sources providing an overall picture of the event
- 4) **Official Alert:** A notification posted by an official government or private sector source

4.9 Credible Sources for Corroboration

First Tier – A first tier source is one that does not typically need additional corroboration prior to release. Sources that construct the first tier platform include major news networks, such as CNN and Fox; major newspapers, such as USA Today and The Washington Post; and international news, such as the BBC and The International Herald Tribune. These sources *do not typically need additional corroboration prior to release:*

- Major news networks (Television and Internet)
 - CNN, FOX, ABC, NBC, CBS, MSNBC, Associated Press, Reuters (local affiliates of these major networks can be considered Tier 1 sources)
 - Local affiliates of major networks, preferably sourced by the wire services like AP or Reuters
- Major newspapers
 - Washington Post, LA Times, USA Today, US News and World Report, Wall Street Journal, Chicago Tribune, Houston Chronicle, Boston Globe, Arizona Republic, San Francisco Chronicle, Detroit Free Press, Miami Herald
 - Some major local/state newspapers are appropriate as well (New York Daily News, Chicago Sun Times, Minneapolis Star Tribune, Seattle Times, etc.)
- International News
 - BBC, Sky News, UPI (United Press International), IHT (International Herald Tribune), AFP (Agence France-Presse), Asian Times Online, Al Jazeera English, Prensa Latina (Latin American News Agency), The Guardian, Le Monde (France), The Economist, Kyodo News (Japan), The Australian News, German News, Canada Free Press, Agenzia Italia, United News of India, EFE (Spain), ARI (Russian Information Agency),

Other Sources - *Need to be verified by a First Tier source prior to release.*

- Government or specialized sites with a specific focus. Often includes .org's, .net's, and .co's.
 - AllAfrica.com, Emergency and Disaster Management Service, GlobalSecurity.org, etc.
- Obviously partisan or agenda-driven sites (political bias must never be reflected in an IOI)
- Tabloids (national and international)
 - The Sun (UK), National Enquirer, Star, etc.
- Blogs, even if they are of a serious, political nature
- Popular magazines
 - People Weekly, Washingtonian, etc.

- News collection/ compilation sites
 - NationalTerrorAlert.com, Drudge Report.com, DisasterNews.net, Opensourceintelligence.org, Homelandsecurityleader.com, HomelandSecurityToday.com.

4.10 IOI Distribution Lists:

There are different types of distribution lists that the MMC uses. Each one addresses a particular group, depending on the severity of the event. The following is a catalog of the different lists and the purpose of each.

- 1) **Default** – this is a Full Distribution (FULLDIS) List, with more than just NOC personnel listed, that is primarily used for IOIs pertaining to terror attacks/terrorism stories, border/immigration issues, natural disasters, wildfires, floods, drugs/drug violence, mass killings/shootings, domestic oil spills, health concerns, etc.
- 2) **LIMDIS** – this is a Limited Distribution List that consists primarily of certain DHS, NOC, and MMC Leadership. IOIs that are sent utilizing the LIMDIS list are major traffic disruptions, suspicious package/powder incidents, hazmat, and school lockdowns, when it is not clear that the threat is real (e.g.: a forgotten backpack).
- 3) **SN-Only** – this is reserved for the SN team and includes specific members of the DHS Privacy office so that they verify MMC complies with the spirit and intent of the PIA, especially when monitoring Social Media.
- 4) **SPECDIS** – this is a Special Distribution List, which is determined by NOC Leadership and is used in rare cases, unusual events, or for certain individuals, and only when directed.
- 5) **Test** – this is used for training and test purposes.

Note: For a current copy of any of the above IOI distribution lists, please refer to management and request that distribution list be sent to you.

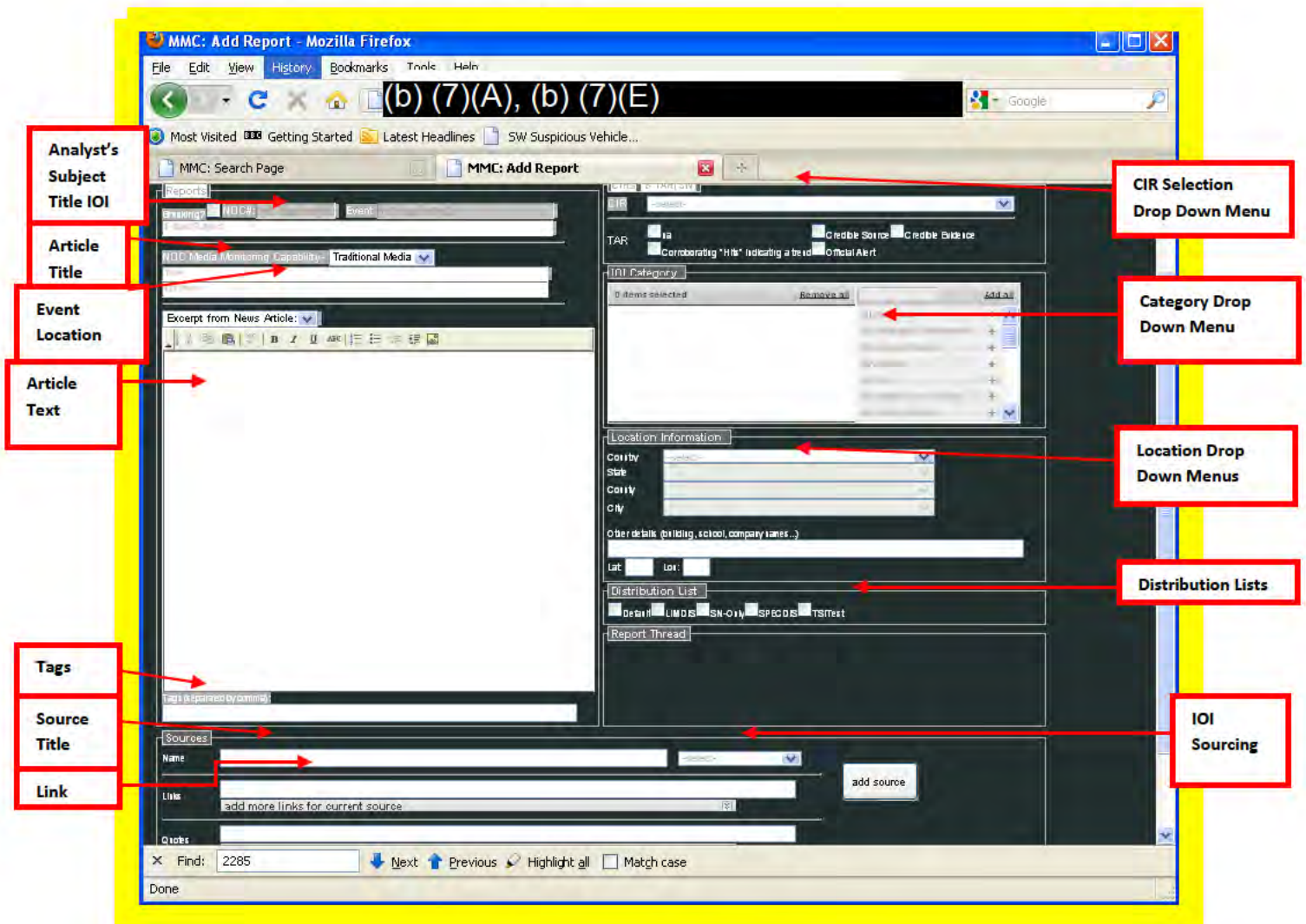
4.11 Creating IOIs (Traditional Media Application)

The MMC team utilizes the App as its regular method for distributing IOIs. The App is a worksheet like function that requires the analyst to input data into specific fields, resulting in a correctly formatted IOI once published. The App automatically databases each item that is distributed, which results in an automated numbering of distributions. This means that when creating an IOI, the new report will be sequentially numbered, building on previous distributions. When analysts are generating an update for an IOI, they only have to make sure that they are updating the correct string (incident) and the App will automatically ensure that it is correctly numbered.

Analysts are responsible for:

- Generating a subject line that summarizes the main points of the article in a clear and concise manner and entering it in the proper field
- Copying and pasting the article's original title into the proper field
- Selecting the correlating category(ies)
- Selecting the most specific location possible from the drop down menu
- Copying and pasting relevant points from the article into the text field
- Identifying the specific media source and entering it in the proper field

- Copying and pasting the source link into the correct field
- Selecting the method used to find the article (Sourcing)
- Inserting tags (keywords)
- Selecting correct distribution list (Default, LIMDIS, SPECDIS)
- Proofing the entire report
- Verifying that the format is correct
- Ensuring that no PII is included except when authorized by the approved NOC MMC PIA dated Jan 6, 2011
- Verifying it is operationally relevant and compliant with the Media Monitoring Guidance Reminder memo

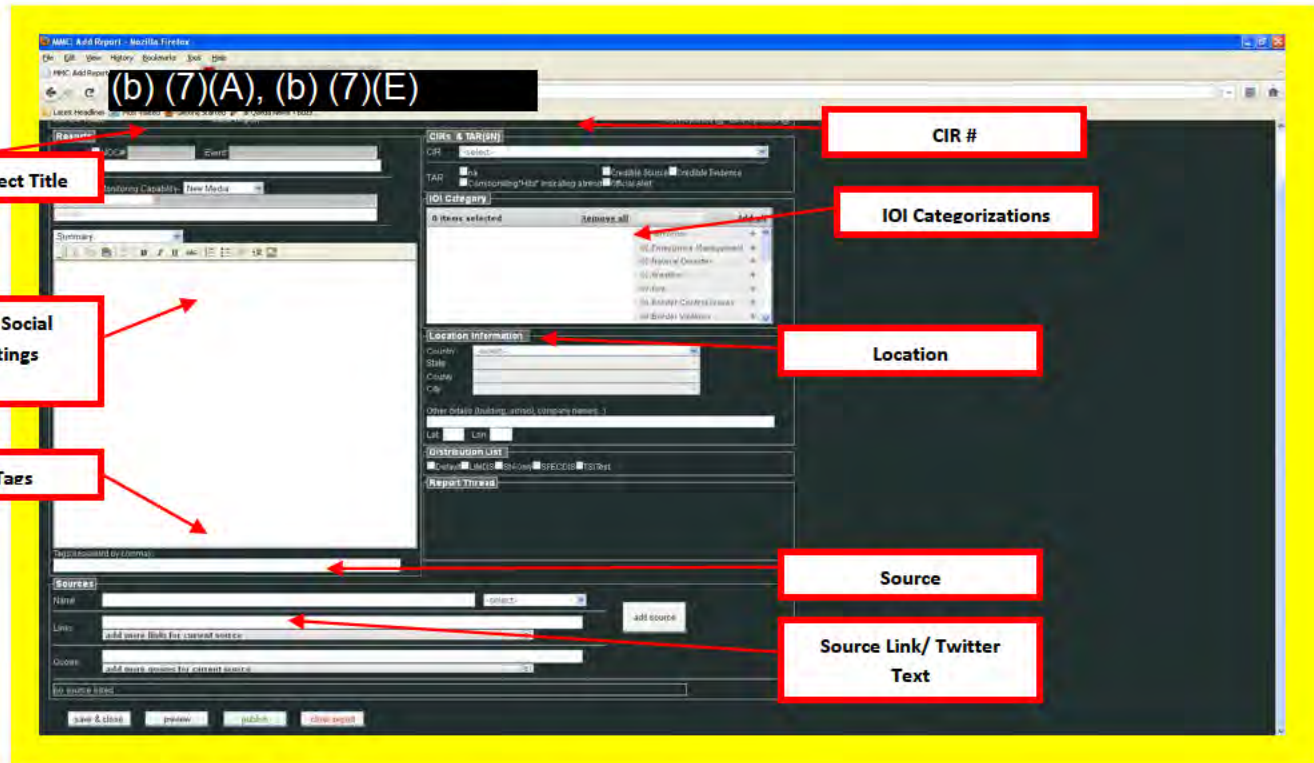


4.12 Creating IOIs (Social Media Application)

The SN team utilizes the App as its regular method for distributing IOIs. The App is a worksheet like function that requires the analyst to input data into specific fields, resulting in a correctly formatted IOI once published. The App automatically databases each item that is distributed, which results in an automated numbering of distributions. This means that when creating an IOI, the new report will be sequentially numbered, building on previous distributions. When analysts are generating an update for an IOI, they only have to make sure that they are updating the correct string (incident) and the App will automatically ensure that it is correctly numbered.

Analysts are responsible for:

- Generating a subject line that summarizes the main points of the article in a clear and concise manner and entering it in the proper field
- Selecting the correlating category(ies)
- Selecting the most specific location possible from the drop down menu
- Pulling relevant points from multiple social media sources and generating a concise summary in the text field
- Identifying the social media sources and entering them in the proper field
- Copying and pasting the source links/social media postings into the correct field
- Selecting the method used to find the article (Sourcing)
- Inserting tags (keywords)
- Selecting the correct distribution list(s) (Default, LIMDIS, SPECDIS, SN Only)
- Proofing the entire report
- Verifying that the format is correct
- Ensuring that no PII is included except when authorized by the approved NOC MMC PIA dated Jan 6, 2011
- Verifying it is operationally relevant and compliant with the Media Monitoring Guidance Reminder memo

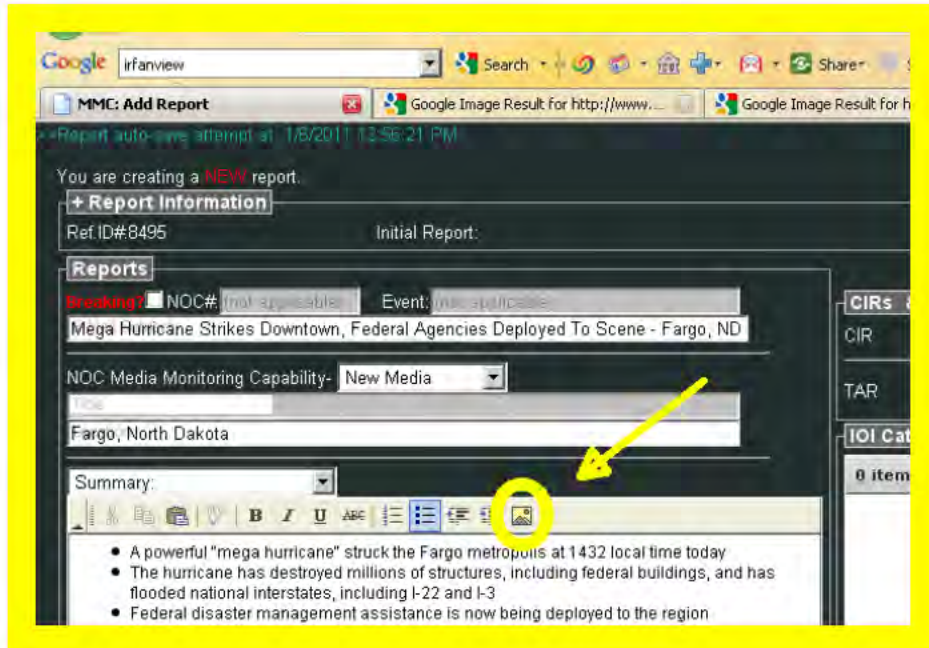


4.13 Application – IOI (Uploading Images):

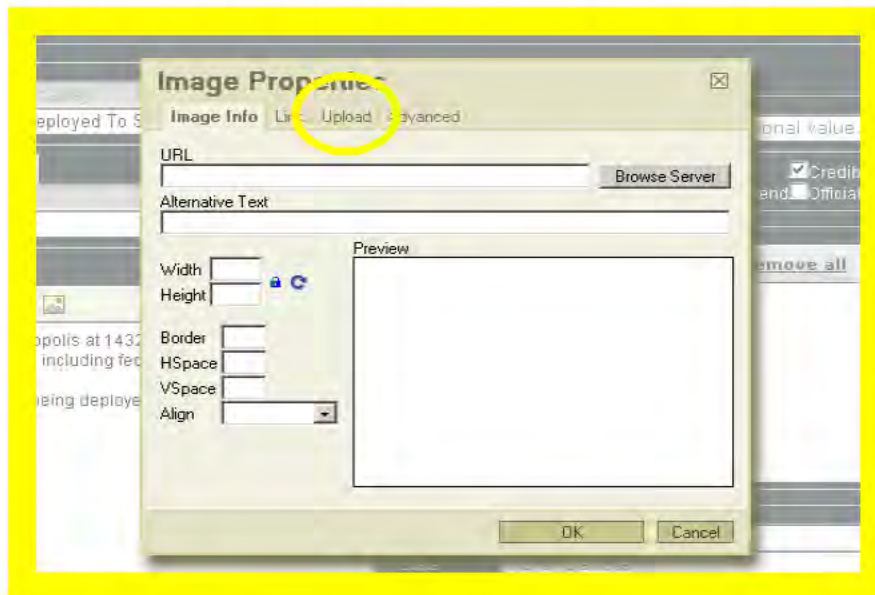
A valuable resource in shaping the operational picture of the DHS NOC and senior level staff is the use of photographs of an event or incident. Analysts can easily upload pictures from Social Media and Traditional Media sources to add an extra layer of operationally valuable information to each report.

Utilize the following procedures to upload photographs to IOIs in the MMC Application:

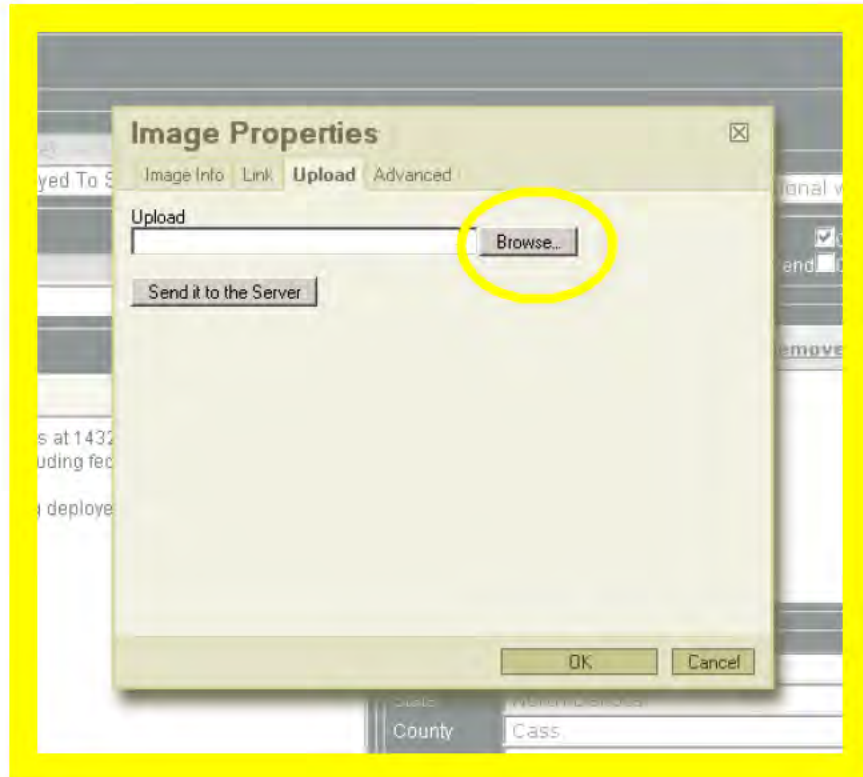
- 1) Right click on the photo that you would like to use and select “save image as”. You will need to save the photograph on one of the office shared drives in order to access it for upload to the App. Use the naming convention **XXYYZZ-File-Name.jpg** when saving photos for use in reports. *Example: 121910-Iowa-Road-Closures.jpg.*
 - MMC Shared Drive address: (see account information sheet)
 - SN Shared Drive address: (see account information sheet)
- 2) In the report page on the Application, click on the picture icon above the report text box.



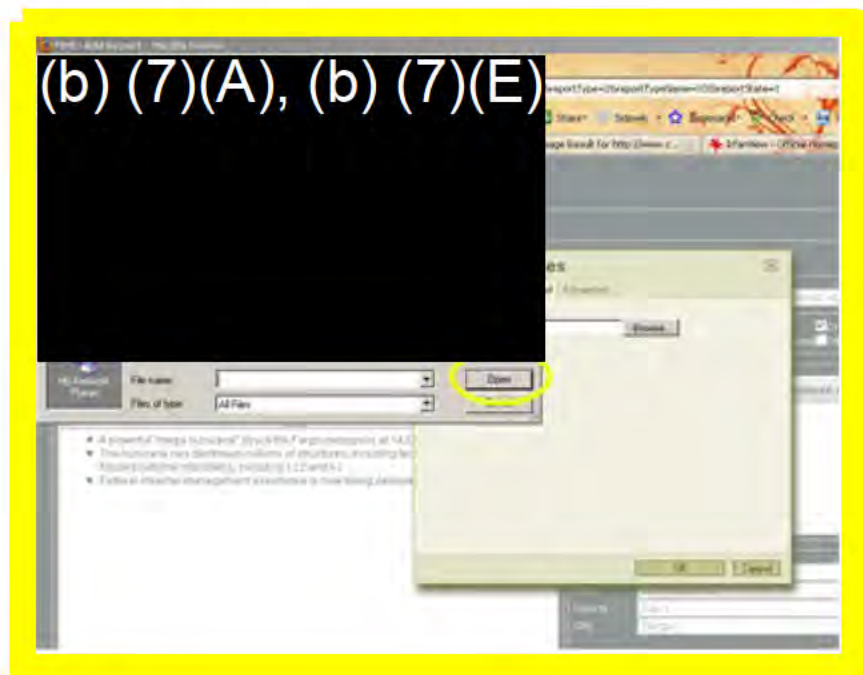
3) When the “Image Properties” window appears, select the “UPLOAD” tab at the top.



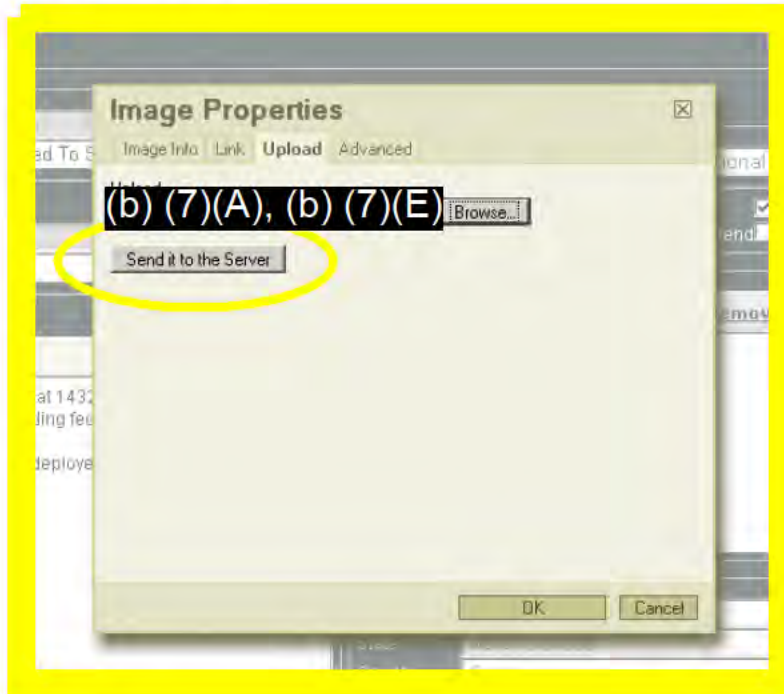
4) Click on the “BROWSE” button.



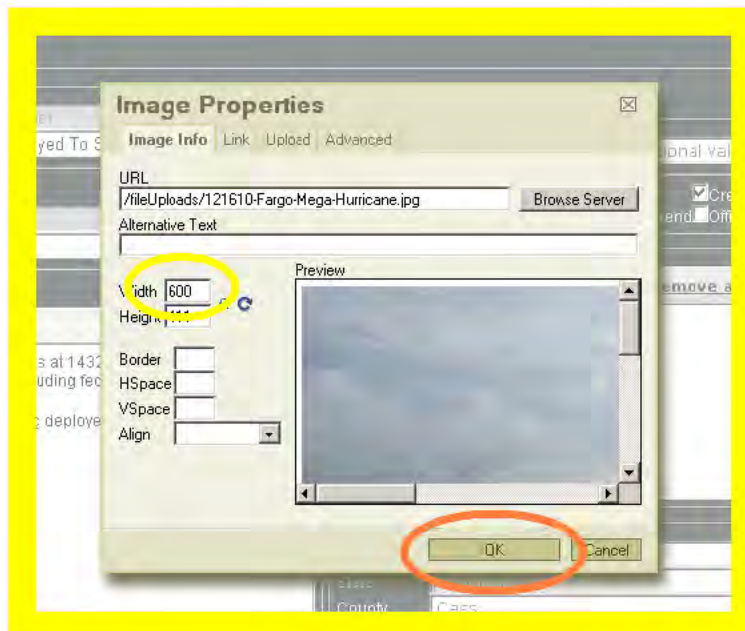
- 5) After selecting BROWSE, a window will open, allowing you to locate the file in which you saved the photograph (see account information sheet for shared drive information). Find and select the file, and then click "OPEN"



6) Select "SEND IT TO THE SERVER"

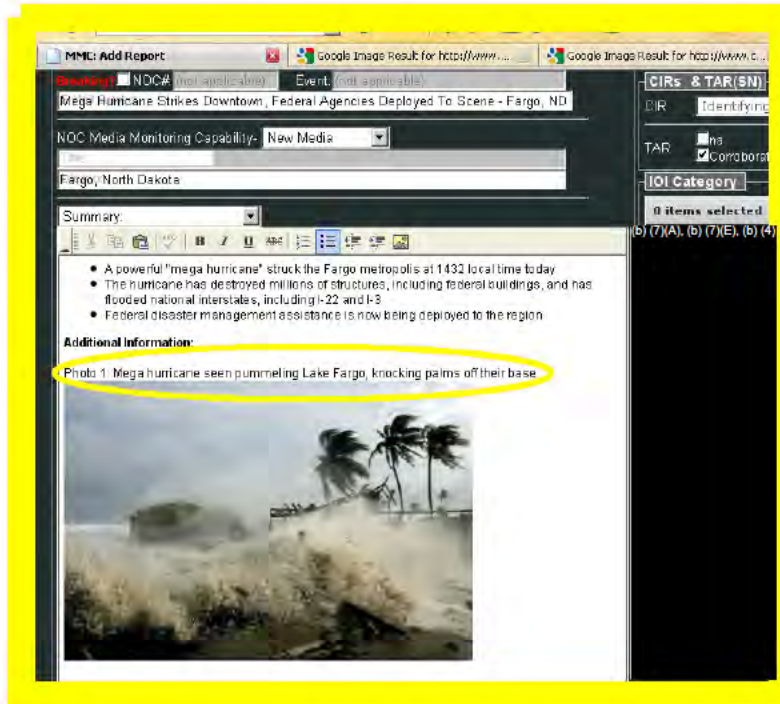


7) Once you select "SEND IT TO THE SERVER", your image will appear in a small preview box. Set the width to 400 and select "OK".



- 8) The image will then appear in the report's text box. Ensure that an **Additional Information** heading is added above the photograph, as well as a brief caption identifying the image.

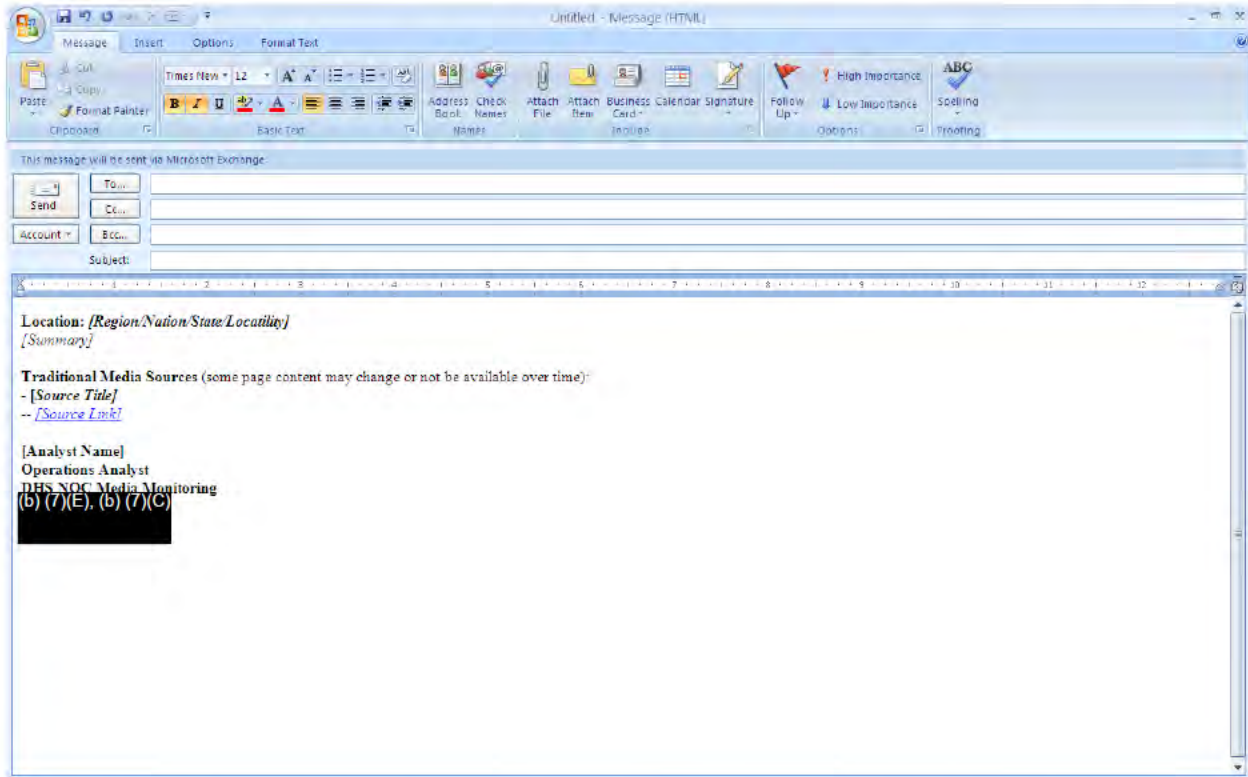
Example: Image 1: Waves From Hurricane Fred Breaking On A Beach In Florida



4.14 Outlook – IOI Backup (Traditional Media):

If the App is unavailable, analysts can generate an IOI via Microsoft Outlook using the following process:

- Open a new message in the Outlook program
- Insert the format text into the message or type layout. An easy way to get the format is to copy it from a previous IOI
- Generate a subject line that reflects the main points of the incident. When applicable, include a location.
- Add the location of the incident. Ensure this is the actual incident site and not the location of the journalist or news source.
- Insert the article's text.
- Insert the article's source and link.

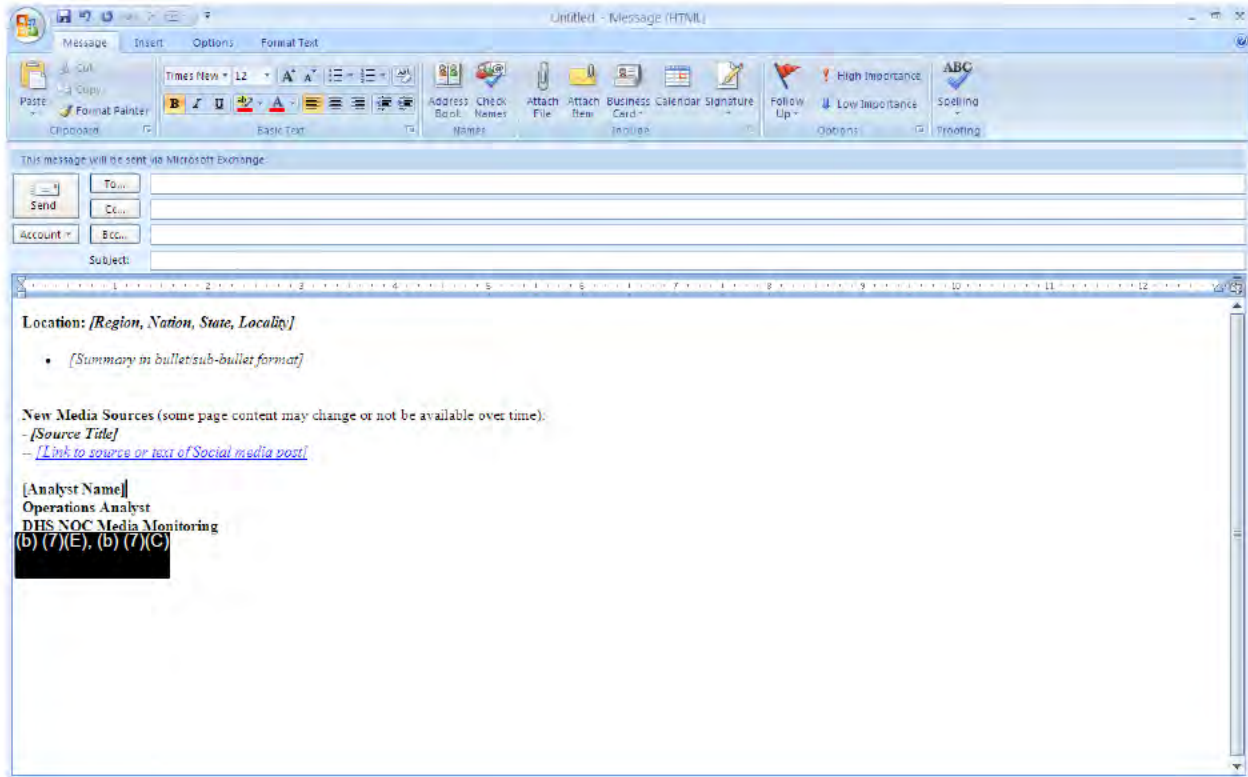


When adding information into the application/email, it is imperative that the analyst reviews the article for internal errors, such as spacing or grammar. Using the preview mode prior to distribution, and then copying and pasting the item into a word document is a simple way to ensure that there are no spelling or grammar issues. Errors can also be checked in Outlook prior to publishing.

4.15 Outlook – IOI (Social Media):

If the App is unavailable, analysts can generate an IOI via Microsoft Outlook using the following process:

- Open a new message in the Outlook program
- Insert the format text into the message or type layout. An easy way to get the format is to copy it from a previous IOI
- Generate a subject line that reflects the main points of the incident. When applicable, include a location
- Add the location of the incident. Ensure this is the actual incident site and not the location of the journalist or news source
- Insert the report text in bullet format
- Insert the sources and links



4.16 IOI Corrections:

Correction notices are issued in the event that incorrect information is distributed in an IOI. The magnitude of misinformation can range from a misspelled word to a missing link. Whenever the analyst finds a mistake in a distribution after the item is sent, the first step the analyst will take is to notify the MMC Watch Lead, and if necessary, contact the MMC Program Manager to inform them of the mistake.

Management will review the severity of the mistake and determine whether a correction notice will be issued. Under no circumstance will the analyst send out a correction notice without managerial approval. If an IOI is numbered wrong, a correction notice usually is not issued. Update the log with the correct IOI number and ensure the succeeding IOI is correctly numbered.

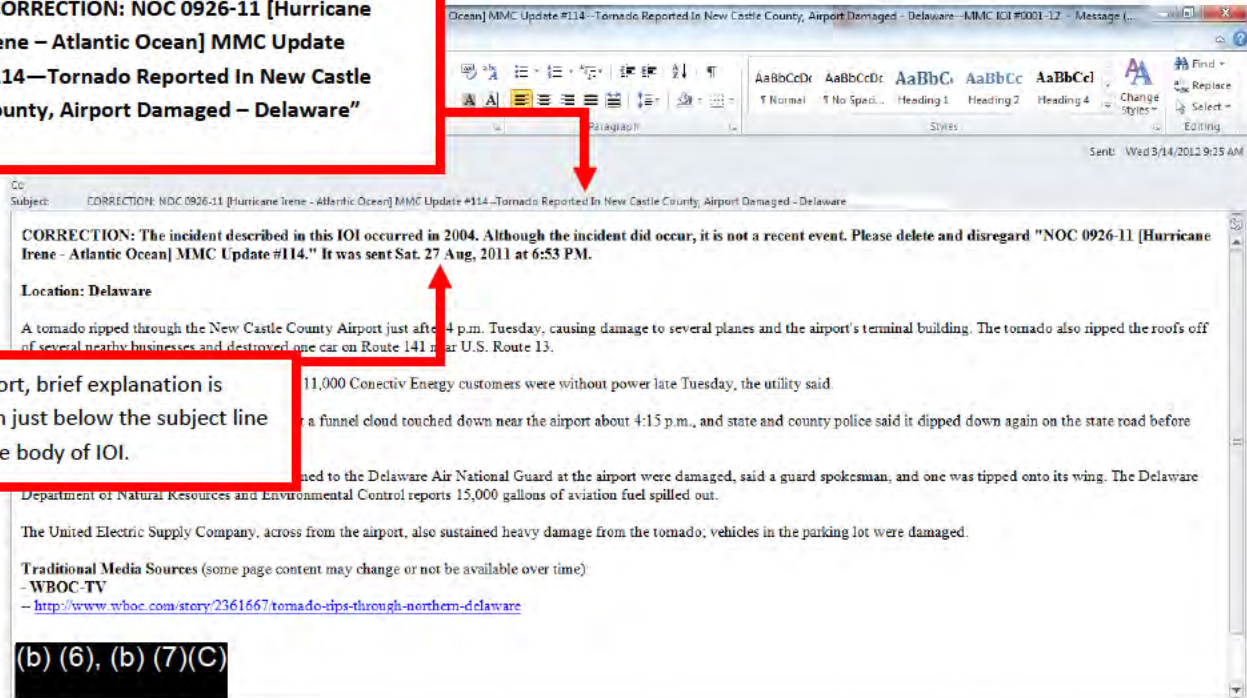
It should be noted that although MMC strives to send high quality work, mistakes at times do occur. Taking time to thoroughly review an IOI prior to distribution and maintaining a high degree of attention to detail will keep mistakes to a minimum. When a correction notice is required, the analyst will draft a brief summary detailing the error and providing corrected information. This summary will be bold and placed at the top of the IOI, before the rest of the report. The word **CORRECTION:** will also be placed at the beginning of the IOIs subject line.

*Sample Subject Line: **CORRECTION: NOC 1196-10 [H1N1 Flu - United States] MMC Update #709--Pennsylvania Confirms 125 Total H1N1 Flu Cases***

Sample Correction Summary: **CORRECTION: The total number of deaths provided in the subject line for this IOI was incorrect. Pennsylvania has confirmed 125 total flu cases, not 125 total flu deaths. The information has been corrected in this notice.**

Subject line should now read:

“CORRECTION: NOC 0926-11 [Hurricane Irene – Atlantic Ocean] MMC Update #114—Tornado Reported In New Castle County, Airport Damaged – Delaware”



After a correction notice is issued, it should be recorded in the daily log. The analysts should record the item as a normal distribution, but also include the reason that the correction was sent in the “Watch Notes” section.

5 The Common Operational Picture (COP 3.1)

The Common Operational Picture is a database used by NOC personnel and Emergency Operations Centers to easily view updated information on incidents being monitored by DHS. The COP serves as a single location in which all of the information regarding actively tracked incidents of significance (Monitored or higher) is collected.

The Media Monitoring Interface can be accessed using Internet Explorer or Mozilla Firefox. The following is the URL for the login screen:

(b) (7)(A), (b) (7)(E)

An alternate method is to access the Executive View via HSIN and then select “COP Operator Applications.” This should bring you to the same log in screen as the URL detailed above.

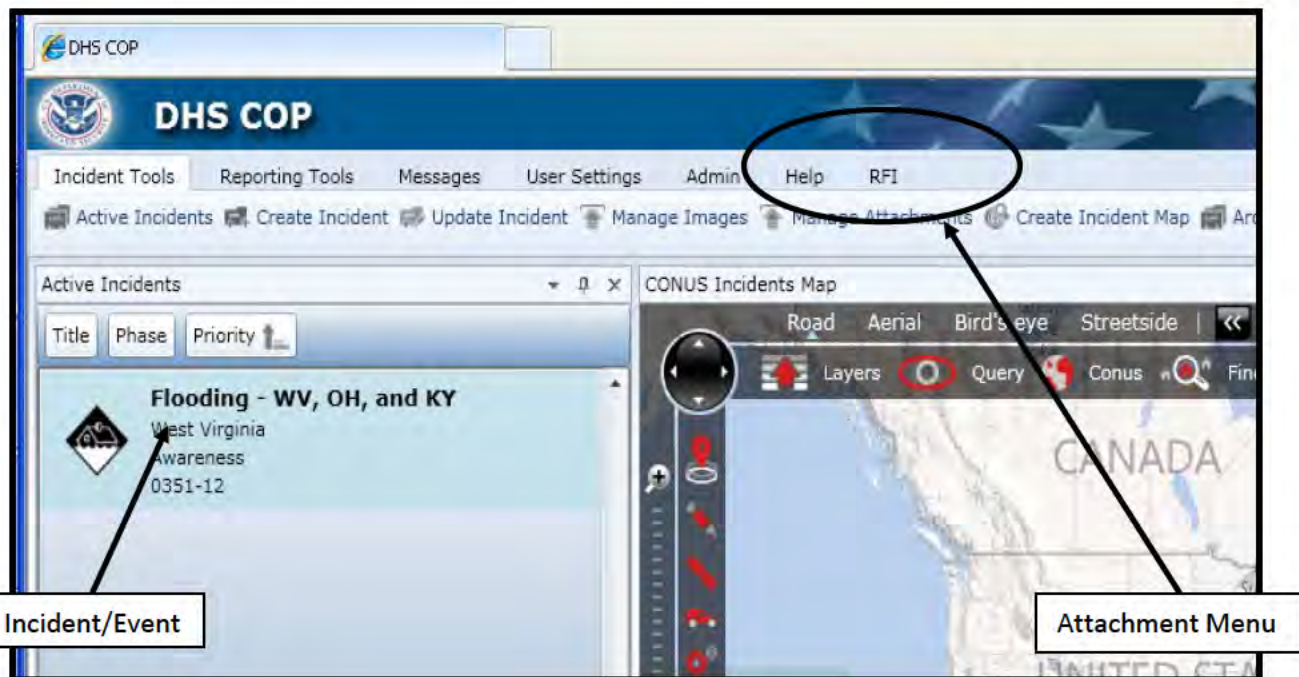
A primary responsibility of the MMC is to update the COP with reports (IOIs) sent out on Monitored or higher items. After the Watch Analyst distributes a new IOI for an event being

tracked under a NOC-assigned number, he/she will add that report to the COP. The following paragraphs outline the instructions for completing this task.

5.1 MMC COP Operations

The MMC monitors the COP 24/7 and is aware of any incidents the NOC is monitoring. They are in constant communication with the NOC and are postured to provide additional content related to the incident in the form of file copies of distributed Items of Interest (IOI) and/or associated image files. The location of this additional content is the “View Reports Tab” of the specific incident Overview window. This process shall be in effect for all incidents from Monitored through Phase III. For this purpose, MMC Analysts will be accorded KMO privileges. The procedure below is to be followed:

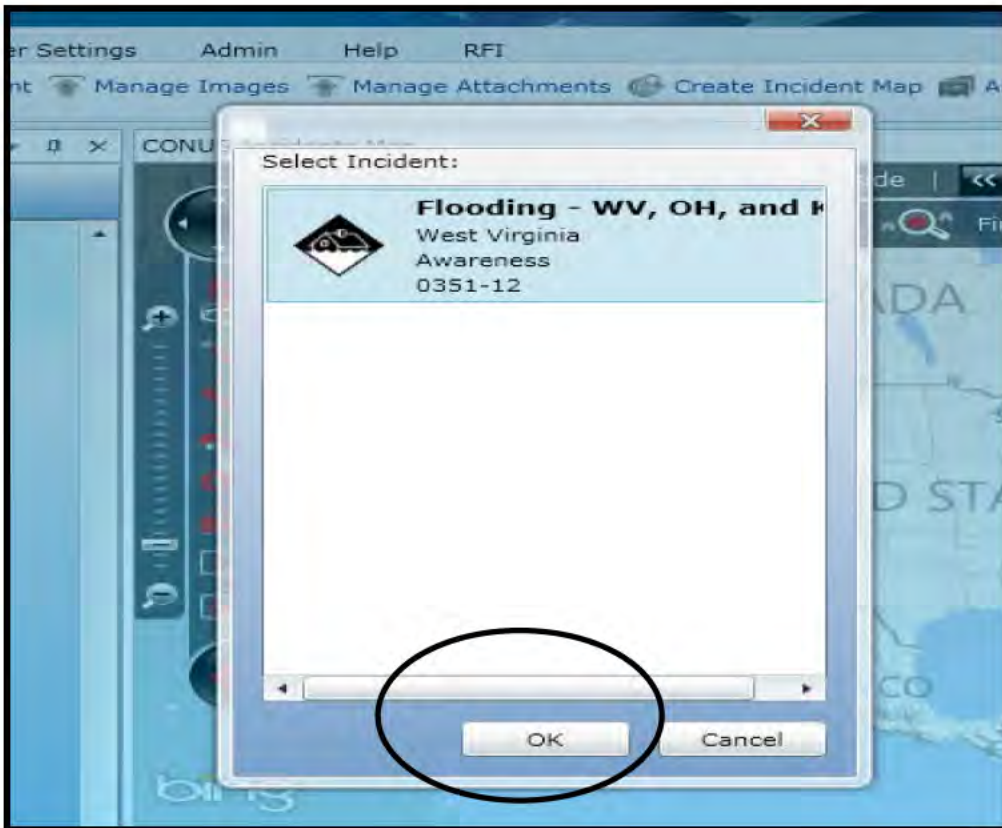
1. Maintain liaison with the NOC and monitor the COP for new incidents
2. When new (Monitored or higher) events are generated, provide additional content in the form of Attachments (see Figure 20) to the Incident based on related IOIs (IOI message saved as file type MHT). If applicable, this shall include the IOI that precipitated the NOC's actions



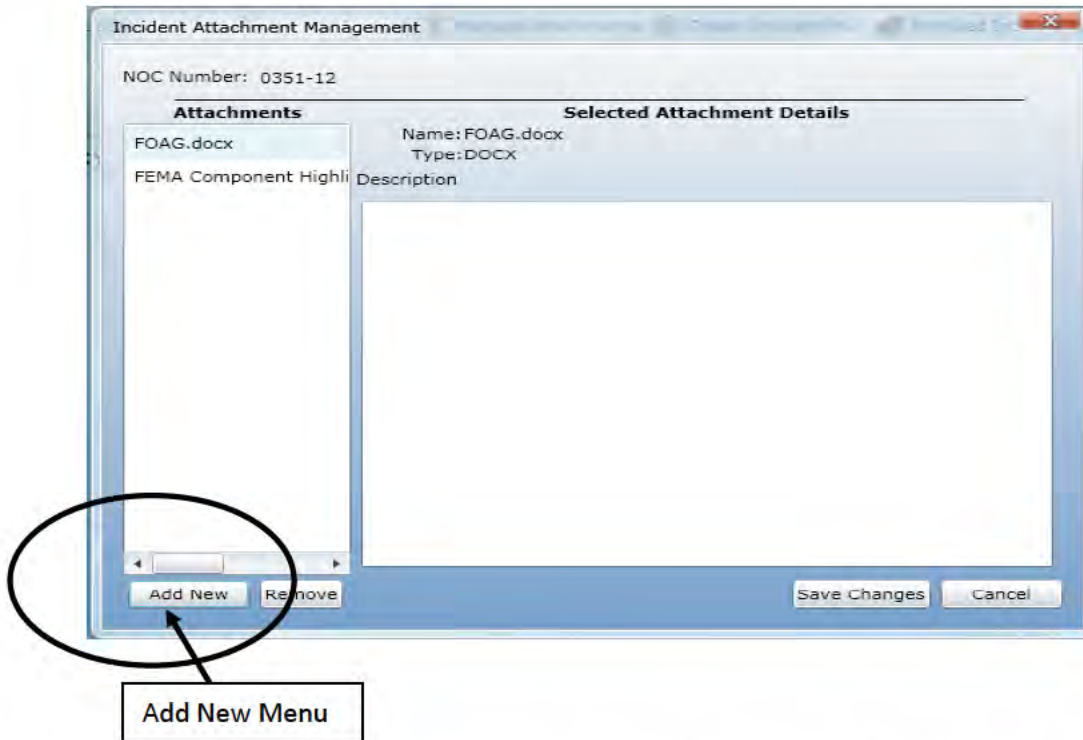
3. Continue adding appropriate related material until the incident is archived
4. Sign into COP using HSIN credentials (Internet Explorer only; if a dialogue pops up asking if you want to display mixed media, click yes)
5. File attachment process
 - 5.1. After distributing an IOI (Monitored or higher) save it as file type “mht.” Save it to the MMC Shared drive: mmc on (b) (7)(A), (b) (7)(E) Report Uploads. Right click, save as, and use the following format for the filename:

MMC Report - Descriptive subj line (analyst's subj line) - Date - Time (5Mar12 - 1504EDT) e.g. MMC Report - Flood Waters Breach Fargo Dikes - 15Mar12 - 1504EDT

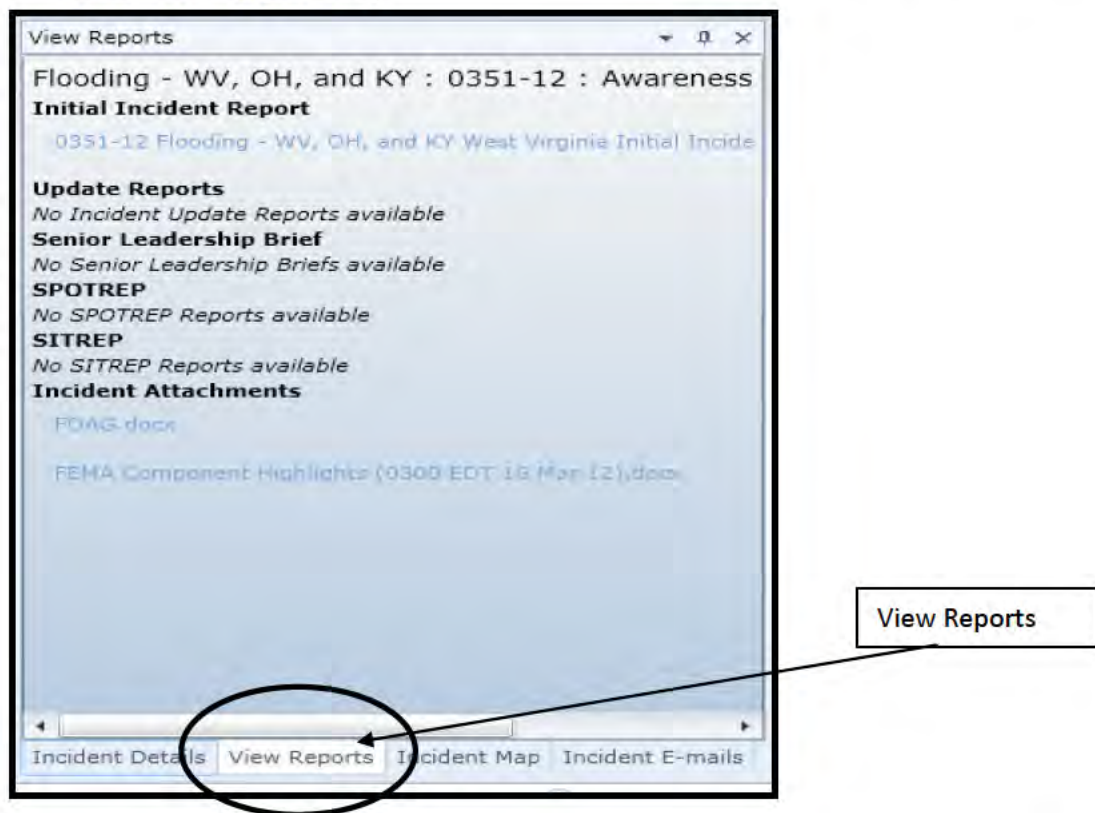
- 5.2. Select COP Incident Tools – Manage Attachment Menu option
- 5.3. Highlight Incident – Select OK (see Figure 21)



- 5.4. Select Add New and navigate to your saved IOI or image file (see Figure 22).
Double click or highlight and select Open



5.5. Save Changes then close out of “Incident Attachment Management” box and verify file is correctly loaded and available in the Overview Window View Reports Tab (click on the Incident title on the left, then look on the bottom right for the View Reports tab).



6 Personally Identifiable Information (PII):

PII refers to information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual. Before distributing reports, including IOIs, MMC and SN analysts must first identify and carefully consider any PII information in media sources before making a decision on whether to preserve such information in distributed reports. In most cases, analysts are required to remove PII in the interest of protecting personal privacy. In a limited number of cases, however, in accordance with the approved NOC MMC PIA dated Jan 6, 2011, analysts are authorized to include PII in a distributed report. Guidance on when and how make such determinations on PII is addressed in the following paragraphs and is based on the current PIA which is the final authority.

In most circumstances, analysts will not report PII for private citizens (i.e., people who are not prominent government officials or news media personalities, regardless of whether they are witnesses, victims, observers or in some other way connected to an event covered in an IOI or other report product. There are, however, rare "*in extremis* situations" when it may be permissible to use PII for private citizens. An *in extremis* situation occurs when there's an imminent threat of loss of life, serious bodily harm, or damage/destruction to critical facilities or equipment. In these circumstances, the appropriate DHS OPS authority must approve PII, in which case MMC management would need to be made aware of the situation. (DHS OPS authority includes OPS Senior Executives and the SWO.)

Generally, PII for public officials or spokespersons may be reported when it adds value and lends credibility to a report or facilitates coordination with federal, state, local, tribal, territorial, foreign, or international government partners. The MMC will not report on high-profile people such as celebrities, sports figures or media members who are victims unless they are current or former public officials. Lastly, it is important to note that the MMC must never report on individuals suspected or accused of committing crimes of national or homeland security interest if captured (unless they are killed or found dead).

In accordance with the NOC MMC PIA dated Jan 6, 2011, PII is authorized in reports for:

- 1) U.S. and foreign individuals *in extremis* situations involving potential life or death circumstances;
- 2) Senior U.S. and foreign government officials who make public statements or provide public updates;
- 3) U.S. and foreign government spokespersons who make public statements or provide public updates;
- 4) U.S. and foreign private sector officials and spokespersons who make public statements or provide public updates;
- 5) Names of anchors, newscasters, or on-scene reporters who are known or identified as reporters in their post or article or who use traditional and/or social media in real time to keep their audience situationally aware and informed;
- 6) Current and former public officials who are victims of incidents or activities related to Homeland Security; and

- 7) Terrorists, drug cartel leaders or other persons known to have been involved in major crimes of homeland security interest (e.g., mass shooters such as those at Virginia Tech or Ft. Hood) who are killed or found dead.

PII in these cases may include: names; affiliations; positions or titles; and publicly-available user IDs and contact information for *in extremis* situations (case 1) only.

6.1 Privacy Impact Assessment

- See SOP Appendix A

6.2 Quality Control

The MMC employs a vigorous Quality Control process to ensure that PII is not inadvertently included in reports. IOI reports are reviewed at multiple steps throughout the production process, and checks are also completed after the report has been distributed. While a report is being generated, it is reviewed at least twice, once by the analyst generating the report, and then again by his/her counterpart. Every IOI is checked by the shift's Watch Lead prior to distribution. All IOIs distributed during each 24-hour period are checked by an MMC Senior Reviewer during the production of the MMC's Operational Summary. The MMC's Quality Control leads also conducts a weekly review of all reports distributed to ensure that any potential PII inclusions missed by personnel on watch are identified and corrective action is taken. Privacy Compliance Reviews (PCR) are also conducted approximately every six months to ensure all aspects of the MMC program are completely compliant with letter and spirit of the PIA.

6.3 Inadvertent PII (Redaction)

When PII is inadvertently included in an MMC distribution, there is a multi-step notification and redaction process that must be implemented to ensure that reports are corrected in accordance with the MMC PIA.

In the event of an inadvertent PII inclusion in MMC reports (IOI, Awareness, Phase, OPSUM, Weekly Data Reports, etc.), the following procedure must be implemented to fully comply with PII guidance and rules.

As soon as unauthorized PII has been identified, the analyst must notify MMC leadership who will notify the DHS/OPS NOC Director that an IOI with inadvertent PII included had been sent and request authorization for the watch to send an email deletion advisory to the full distribution list and an email to the MMC team notifying them that the PII must be deleted from the errant IOI.

A second email will advise readers that unauthorized, but unclassified information was accidentally included in the IOI (identified by subject line and DTG) and therefore must be permanently deleted. A general description of how to remove the PII or permanently delete the IOI in MS Outlook will be provided along with a notice to contact the recipients' system administrator with questions for programs other than Outlook.

7 Operational Summary (OPSUM):

Night shift analysts will compile a summary of items that have been distributed by the MMC over each 24 hour period. The Operational Summary provides a synopsis of distributed items based on a set of designated priorities that are generated by the NOC. In rare circumstances, the NOC may require that Operational Summaries be generated at irregular intervals in support of ongoing situations. These special reports will be generated at the direction of the NOC or senior personnel, and will be closely coordinated with the senior reviewer before distribution. In all cases, the OPSUMs and Special Reports NEVER include PII except when authorized by the approved NOC MMC PIA dated Jan 6, 2011

The on-duty Traditional and Social Media analysts will collaborate to generate a single report and then submit it to the designated Senior Reviewer no later than 0400. The Senior Reviewer will check the report for proper grammar, punctuation, content, PIA compliance, and adherence to the NOC Priorities. Once the Senior Reviewer has approved the Operational Summary, the on-duty Traditional Media Watch analyst will distribute it.

- One copy of the OPSUM will be sent to the IOI Distro List using the BCC line.
- A second (identical) copy will be sent to:
 - WHSR (see account information sheet) in the TO Line
 - All senior reviewers and the DHS/OPS Senior Advisor in the BCC line
- The OPSUM should be distributed as soon as it is checked by both watch analysts, after receipt from the Senior Reviewer, and no later than 0500 unless an early production call is issued by the NOC. If an early production is requested the on duty analysts are responsible for notifying the Senior Reviewer as soon as possible that the time production time has been adjusted.

7.1 Operational Summary (OPSUM) Format:

The Operational Summary (OPSUM) is distributed each morning to provide recipients with the most current update for ongoing situations (e.g. Phases, Awareness), and events of high media interest. As such, the OPSUM format directly reflects the published NOC Priorities. Analysts will gather the most current media information on active situations for the summary. The most current information is considered information not older than 24 hours and will include information from previous IOIs in addition to scanning for new information and relevant updates. It is important to remember that the Operational Summary is used for agency briefings and must relay the most current information in a structured and easily readable format.

Note: If there was a NOC item during the previous 24 hours that was closed out prior to the drafting of the morning OPSUM, it may be included if there was significant coverage by the MMC or heavy interest on part of the NOC while the item was active.

- The OPSUM is created in an Outlook email message.
- The standardized subject line is used for the report.
- A short summary of the topics covered in the report will also be included in a header for the OPSUM.
- Analysts will utilize a header and bullet format when inputting information.

- To distinguish between Traditional and Social Media items, all Social Media input will be italicized. Social Media analysts will also include *(Social Media)* at the end of each bullet as an additional designator if the content under one priority is mixed with information from Traditional Media
- If all the bullets under a priority are from Social Media, then the *(Social Media)* tag should only be included next to that specific priority title.
- Hyperlinks to sources will be included with the bullets for items of high interest or particularly significant summaries. SN analysts will include links to translated articles if using foreign language sources.

Example Operational Summary provided on the following pages.

NOC MEDIA MONITORING OPERATIONAL SUMMARY (OPSUM)
 24 Hour Summary, August 16, 2011

TODAY'S OPSUM COVERS THE FOLLOWING NOC PRIORITIES

- **NOC Priority Items with new information**
 - [Southwest Border Events with U.S. Homeland Security Implications](#)
- **Other Significant Items**
 - [Severe Weather – KY/IN](#)
 - [Al Qaeda Urges Attacks Against U.S.](#)
 - [Continued Violence in Syria](#)
- **NOC Priority Items (Nothing Significant To Report (NSTR))**
 - Global/Commercial Aviation Cargo Threats/Incidents Targeting U.S. Interests
 - Mass Migration in the Caribbean with U.S. Homeland Security Implications
 - CBRNE Threats/Incidents Targeting U.S. Interests

NOC 0003-11: Southwest Border Events with US Homeland Security Implications

Killings (non U.S. persons)

- The Mexican Army captured the suspected leader of a Beltran Leyva drug cartel who allegedly controlled drug trafficking in the Costa Grande region of Guerrero state and orchestrated a number of killings [Fox News Latino](#)
 - The suspect had taken over the Beltran Leyva cartel's operations in the city of Zihuatanejo, Guerrero, after the arrest of one of his bosses, unleashing a wave of executions of rival group members
- *Three separate grenade attacks in Mexican cities over the weekend have resulted in 1 death and 7 injuries (Social Media) [Milenio News \[Translated by Google\]](#)*
 - *The attacks occurred at a prison in Apodaca, Nuevo Leon; on a busy tourist boulevard in Veracruz; and at a movie theater in Reynosa (Social Media)*
- *The director of the Ixtlahuacán del Río Police was executed on Saturday night in an ambulance in the municipality of Cuquio (Social Media) [Guerra Contra El Narco \[Translated by Google\]](#)*
 - *Medical staff confirmed that the vehicle was intercepted by an unknown number of individuals on the Río-Cuquio Ixtlahuacán highway at San Juan del Monte (Social Media)*
 - *The murderers beat emergency medical technicians after the execution and fled (Social Media)*

Other Impacts of Southwest Border Violence (SWBV)

- As part of the Central American Law Enforcement Exchange, law enforcement officers from Latin America are training with local police in Los Angeles on combating international gang crimes, especially narcotics trafficking, kidnapping and human trafficking
 - The Exchange features a week-long training class made up of about 30 officers from the U.S., El Salvador, Panama, Costa Rica, Honduras and other countries.
 - FBI Officials said Los Angeles stands to benefit from the collaboration because the gang has between 5,000 and 7,000 members.

[\[Back to top\]](#)

OPSUM

Single space between Sections

Hyperlinks take reader to corresponding sections

Items Identified on NOC Priorities but not reported by MMC/SN

Sources Included for Bullets Including significant information

(Social Media) designates contributions from SN Sources. NOT BOLD

Link takes reader back to top of report

OTHER SIGNIFICANT EVENTS:

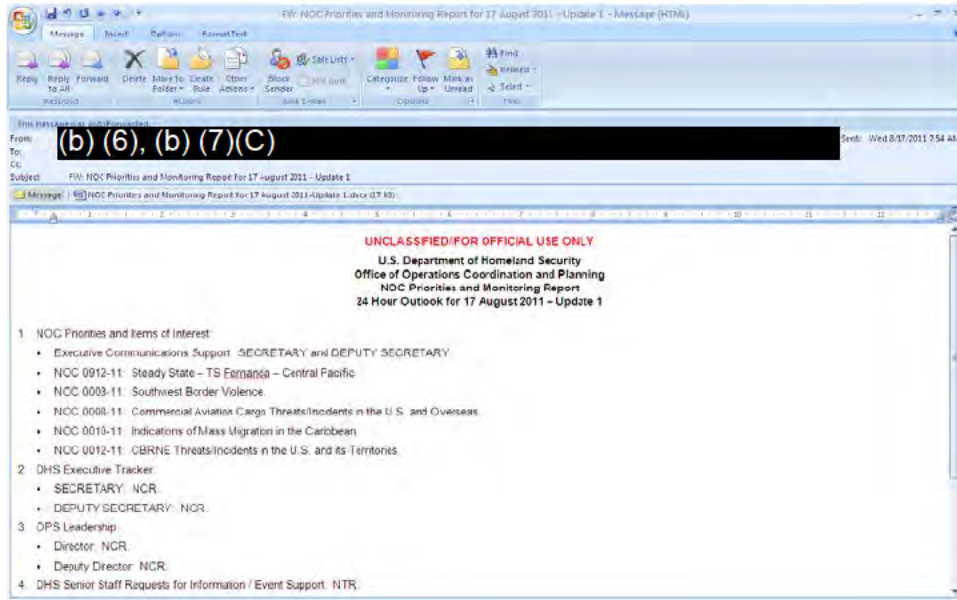
Severe Weather—Kentucky / Indiana (Social Media) [Twitter \[WAVE 3 News\]](#)

- As of 3:00 a.m. [16 Aug] local time, LG & E's outage map was reporting less than 12,000 customers without power in Jefferson County, down from a peak of over 128,000 Saturday night
 - LG & E hopes to have a majority of customers back up and running Monday and Tuesday, and the remaining by Wednesday
 - The Jefferson County Public School system cancelled all classes on Monday due to power outages in the area

Figure 191: OPSUM Continued

8 NOC Priorities:

The National Operations Center publishes a daily NOC Priorities report every 24 hours to identify the priorities for each shift and help guide the information gathering activities of NOC personnel. This report is usually distributed via email from the NOC between 2000-2300 each day. Analyst should use the priorities report to direct their reporting and as a guide for the generation of the Operational Summary.



8.1 NOC Priorities (HSIN Retrieval)

These instructions should be utilized as a means of retrieving the National Operations Center Priorities for each shift should there be a malfunction in the automated forwarding system.

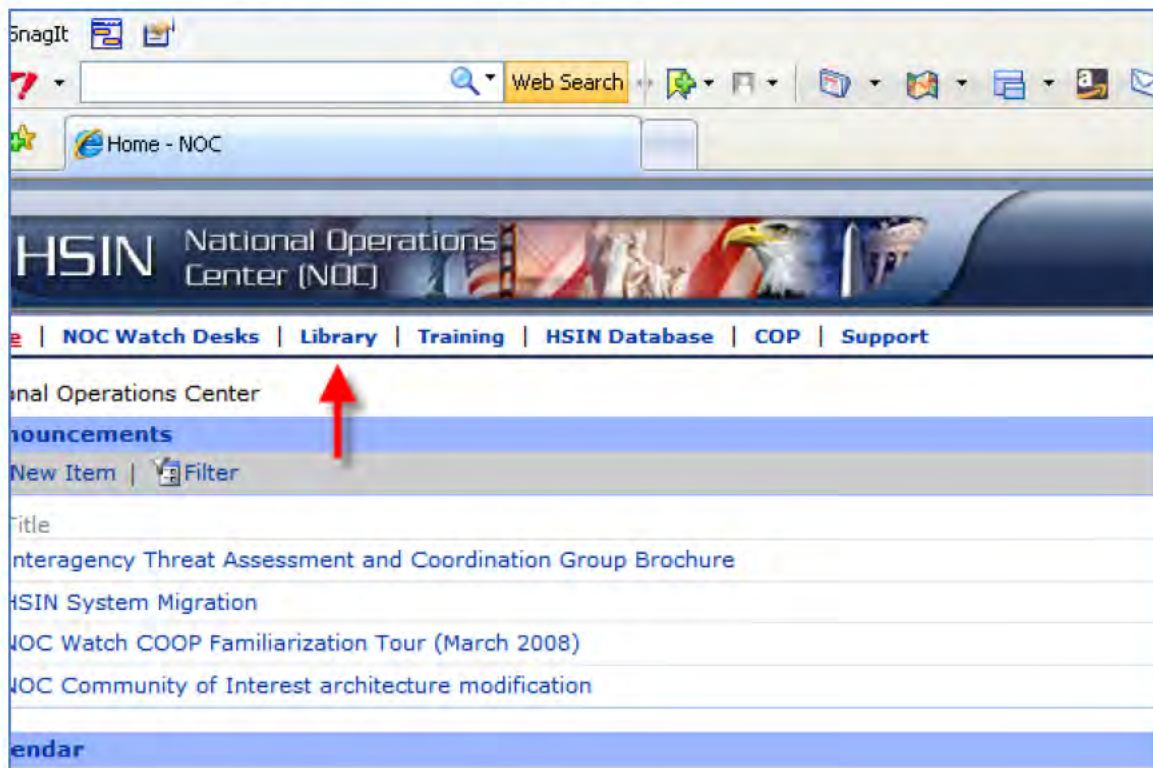
1) Step One: Access the Homeland Security Information Network



2) Step Two: Select the National Operations Center Tab in the lower left corner.

<p>Pager: Other Phone:</p> <hr/> <p>Your Communities</p> <p>Federal -</p> <ul style="list-style-type: none"> Emergency Management Federal Operations HSIN Government Home National Operations Center ←
--

3) Step Three: Select the Library Tab.



4) Step Four: Scroll down to the document library section.

The screenshot shows the National Operations Center website interface. At the top, there is a navigation bar with links: Home, NOC Watch Desks, Library (highlighted in red), Training, HSIN Database, COP, and Support. Below the navigation bar, the page title is "National Operations Center". There are three main sections: "NOC Watch Desk SOPs", "Forms", and "Document Library". The "Document Library" section is highlighted with a blue header and a red arrow pointing to it from the left. The "Document Library" section contains a table with columns "Type" and "Name". The items listed are:

- DHS OPS-HSOC-NOC SA-COP Brief 24 May 06
- The Evolution of HSOC Situational Awareness 03 April 2006 REV4_hurricane_version
- DHS CINT Intelligence Notes
- DHS Cyber Daily Reports
- DHS Daily Ops Report
- FEMA National SITREP
- NOAA Meteorological Update
- NOC Priorities and Monitoring Reports

 Below the table is an "Add new document" button.

5) Step Five: Select the NOC Priorities and Monitoring Reports folder:

This screenshot is a closer view of the "Document Library" section. The "NOC Priorities and Monitoring Reports" folder is highlighted with a red arrow. The "Modified By" column for the first two items is redacted with a black box containing the text "(b) (6), (b) (7)(C)". The "Add new document" button is visible at the bottom of the list. Below the list, there is a section titled "Operations Directorate COOP Documents".

6) Step Six: When the folder opens, scroll down to the **Document Library**

The screenshot shows the HSIN National Operations Center (NOC) website. The navigation bar includes Home, NOC Watch Desks, Library, Training, HSIN Database, COP, and Support. The main content area is titled 'National Operations Center' and contains three expandable sections: 'NOC Watch Desk SOPs', 'Forms', and 'Document Library'. The 'Document Library' section is highlighted with a red arrow pointing to its header. Below the header, there is a table with columns for 'Type', 'Name', and 'Modified By'. The table lists two documents: 'NOC Priorities and Monitoring Report 5 December 2008' (marked as 'NEW') and 'NOC Priorities and Monitoring Report 4 December 2008'. Below the table is an 'Add new document' link. At the bottom of the page, there is a section for 'Operations Directorate COOP Documents'.

Type	Name	Modified By
Word Document	Crisis Action Process Operating Instructions (v.10 as of 17 Apr 07-SWS)	
Word Document	IIMG SOP (02 23 05)	
Word Document	JFO SOP Appendix-Annexes (v55)	
Add new document		

Type	Name	Modified By
Word Document	11000-14 Identification Access Control Card Request	
Word Document	11000-25 Contract Suitability-Security Screening Request Form	
Word Document	3130 DHS Non-Staff Assignment Form	
Word Document	NAC Access Control - Visitor Access Form	
Word Document	NAC Access Control and Visitor Access Procedures (memo 9-26-06)	
Add new document		

Type	Name	Modified By
Word Document	NOC Priorities and Monitoring Report 5 December 2008 NEW	
Word Document	NOC Priorities and Monitoring Report 4 December 2008	
Add new document		

7) Step Seven: Select the NOC Priority list for the desired date:

This is a close-up view of the 'Document Library' section from the previous screenshot. It shows the table with two rows of document entries. Red arrows point to the 'Name' column for both rows. The first row is 'NOC Priorities and Monitoring Report 5 December 2008' with a 'NEW' indicator. The second row is 'NOC Priorities and Monitoring Report 4 December 2008'. Below the table is an 'Add new document' link. At the bottom of the page, there is a section for 'Operations Directorate COOP Documents'.

Type	Name	Modified By
Word Document	NOC Priorities and Monitoring Report 5 December 2008 NEW	
Word Document	NOC Priorities and Monitoring Report 4 December 2008	
Add new document		

9 Technology Suite

The Media Monitoring Capability is located off the DHS campus. The Traditional Media and Social Media watch desks share a space equipped with an advanced audio video package, allowing analysts to constantly monitor multiple computer programs as well as television network broadcasts at the same time. The technology suite greatly assists the analysts in identifying the most relevant sources and information to be included in the reports. The analysts must be vigilantly attentive to not inadvertently include PII in the reports. The team relies upon internet and cable/satellite for most of its information retrieval. Internet/Cable/Satellite connectivity is provided via commercial contracts. Four large Plasma TVs and computers with multiple screens on each desk enable MMC analysts to perform several tasks (e.g., process video, monitor news broadcasts, compose e-mail) simultaneously.

- The current suite of equipment on the Traditional Media desk includes one Dell Optiplex GX620 workstation (232 GB HD/2MB RAM), one MAC desktop workstation, and three 22" flat screen monitors, and individual analysts are issued a laptop that is used to augment the PCs and to provide a remote capability for surge operations, inclement weather, or other exigencies.
- The current suite of equipment on the Social Media desk includes one MAC desktop workstation, two 19" flat screen monitors, and individual analysts are issued a laptop that is used to augment the PCs and to provide a remote capability for surge operations, inclement weather, or other exigencies.
- Four 40" Samsung flat screen TVs are mounted on a wall in front of the desk and can be viewed from analysts working at either station. The monitors/TVs are equipped with MSI TV Tuner Cards to facilitate radio/TV display and video capture. The system also allows for analysts to change video inputs so that they can display any program that they are utilizing on computers at their desk onto the 40" monitors at the front of the room. This capability helps to facilitate the rapid sharing of information with others in the office as well as display of important information, such as the Common Operational Picture.
- To facilitate communication with the National Operations Center (NOC), the MMC has two phones – a voice over IP phone on each desk and a cellular phone. There is also a pager that the NOC utilizes to disseminate information for ongoing incidents. The MMC office phone is for general business purposes only while the cell phone is used to receive blast calls from the NOC, interact with MMC and NOC personnel, and as a back-up if the landline goes down. The pager is used to receive alerts on NOC Notes, Phase Reports and other related event situations.



MMC Watch Desk



MMC Front of Room Monitors

9.1 Audio Video System:

9.1.1 Direct TV Full Channel List

A&E 265	FINE LIVING 232	Nickelodeon/Nick at Nite (West) 300
ABC Family 311	FitTV 368	Nicktoons Network 302
American Movie Classics (AMC) 254	Food Network 231	Noggin/The N 298
America's Store 243	Fox News Channel 360	Outdoor Channel 606
Animal Planet 282	Fox Reality 250	OLN 608
BBC America 264	FUEL TV 612	ONCE México 415
The Biography Channel 266	Fuse 339	Oxygen 251
Black Entertainment Television (BET) 329	FX 248	QVC 317
Bloomberg Television 353	G4 videogame tv 354	RFD-TV 379
Boomerang 297	Galavisión 404	Sci-Fi Channel 244
Bravo 273	Go!TV 426	Speed 607
BYU TV 374	Great American Country 326	Spike TV 325
Cartoon Network 296	GSN: the network for games 309	Superstation WGN 307
CCTV-9 (Chinese) 455	Hallmark Channel 312	TBS 247
The Church Channel 371	Headline News 204	TCT Network 377
CNBC 355	The History Channel 204	TNT 245
CNBC World 357	History International 271	Travel Channel 277
CNN 202	HITN TV 438	Trinity Broadcasting Network (TBN) 372
Comedy Central 249	Home & Garden Television 229	Turner Classic Movies (TCM) 256
Country Music Television (CMT) 327	Home Shopping Network 240	Turner South* 631
Court TV 203	The Learning Channel (TLC) 280	TV Guide Channel 224
C-SPAN 350	Lifetime 252	TV Land 301
C-SPAN2 351	Lifetime Real Women 261	TV One 241
CSTV: College Sports Television 610	Link TV 375	TVG:The Interactive Horseracing Network 602
Current TV 366	The Military Channel 287	Univision 402
Daystar 369	MSNBC 356	USA Network 242
Discovery Channel 278	MTV 331	VH1 335
Discovery Health Channel 279	MTV2 333	VH1 Classic 337
Discovery Home Channel 286	National Geographic Channel 276	The Weather Channel 362
Discovery Kids 294	NASA TV 376	The Word 373
Discovery Times Channel 285	NBA TV 720	World Harvest Television (WHT) 321
DIY Network 230	News Mix 102	
E! Entertainment Television 236	NRB Network 378	
EWTN 422	NFL Network 212	
	Nickelodeon/Nick at Nite (East) 299	

9.1.2 Direct TV Account Information

Contact MMC Management

9.2 Online Audio-Video Switch

In order to change the channels for the displays at the front of the MMC office, analyst must access the TSI network at: (see account information sheet)

It's probably a good idea to have this interface available during your shift, so that you can make any adjustments on the fly.

Manual Switching

Using the matrix of Inputs (along left side) and Outputs (along top side) you can quickly click which source you would like to display on any one of 5 outputs. Selection is made by clicking the button that references the combination of Input and Output you wish to see, and then click the "Submit" button at the bottom of the page. Outputs 1 through 4 correspond to the TVs left to right, from top row to bottom row:

ONE	TWO
-----	-----

THREE	FOUR
-------	------

Output 5 allows you to assign the audio of any input to the overall room speakers.

Stored Configurations

To make common configurations easily and quickly available, we have set up some presets. By selecting the number from the drop-down menu under “Stored Configurations” and clicking “Load”, you can call up these stored presets. These settings can be changed if we find specific presets that are preferred.

- 1) MMC Extended Desktop HSIN (1), CNN (2), FOX News (3) MSNBC (4).
- 2) MMC Extended Desktop HSIN (2), CNN (1), FOX News (3) MSNBC (4).
- 3) MMC Extended Desktop HSIN (3), CNN (2), FOX News (1) MSNBC (4).
- 4) MMC Extended Desktop HSIN (4), CNN (2), FOX News (1) MSNBC (3).
- 5) SN Extended Desktop HSIN (1), CNN (2), FOX News (3) MSNBC (4).
- 6) SN Extended Desktop HSIN (2), CNN (1), FOX News (3) MSNBC (4).
- 7) SN MAC Desktop HSIN (2), CNN (1), FOX News (3) MSNBC (4).
- 8) SN MAC Desktop (3), CNN (1), FOX News (2) MSNBC (4).

9.3 Mapping Shared Network Drive

To map to MMC’s shared network drives, use the following procedures. When mapping for the first time, you must enter the password (see hard copy of password list in the left pocket of the SOP binder).

For Windows XP computers:

- 1) Click Start
- 2) Click My Computer
- 3) Click on Tools
- 4) Select Map Network Drive
- 5) Select any letter from the dropdown menu for the Drive
- 6) Type in the following under the Folder space for the MMC shared drive
(b) (7)(C), (b) (7)(E)
 - a. For the SN shared drive, type in **(b) (7)(C), (b) (7)(E)**
 - b. The box for “Reconnect at Logon” should be checked
 - c. Do not check the box for “Connect using different credentials”
- 7) Click Finish

For Windows 7 computers:

- 1) Click Start

- 2) Click My Computer
- 3) Select Map Network Drive from the top menu bar
- 4) Select any letter from the dropdown menu for the Drive
- 5) Type in the following under the Folder space for the MMC shared drive
(b) (7)(C), (b) (7)(E)
 - a. For the SN shared drive, type in (b) (7)(C), (b) (7)(E)
 - b. The box for "Reconnect at Logon" should be checked
 - c. Do not check the box for "Connect using different credentials"
 - d. Click Finish

10 HSIN (b) (7)(E) Connection Instructions:

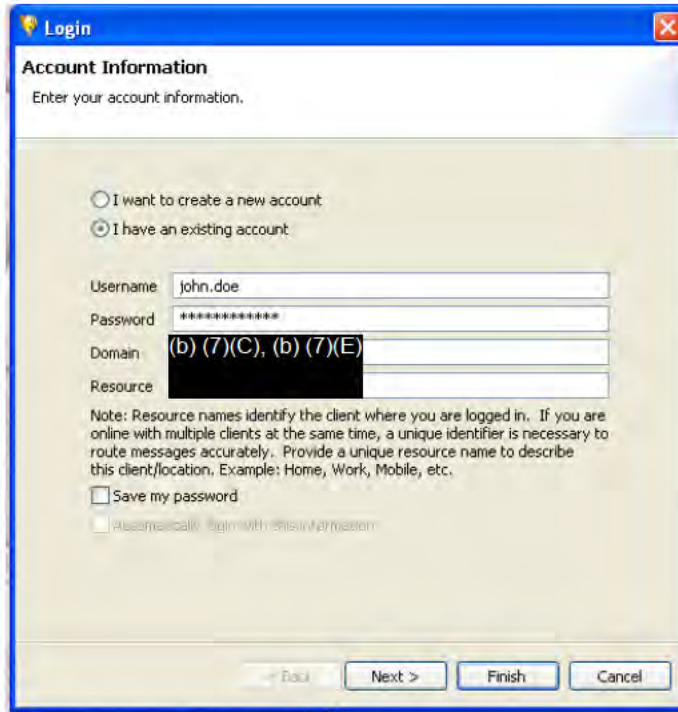
(b) (7)(E) is a text based communications tool utilized by the Department of Homeland Security to connect individuals at different locations. The MMC utilizes (b) (7)(E) as a means to communicate with members of the NOC Watch throughout the shift. The NOC has a dedicated chat room, identified as NOC_Watch in which all members of the NOC Watch team can post information regarding ongoing incidents. MMC analysts will use (b) (7)(E) to pass information on rapidly evolving situations, request information and communicate directly with the SWO, KMO or NDD.

Once logged into HSIN, click on the (b) (7)(E) download box on the right side of the Emergency Management Portal. After selecting the (b) (7)(E) full client download, you will be provided with the (b) (7)(E) EXE file. Once the download is complete, follow each of the instructions given by the prompt windows until the installation process is complete.

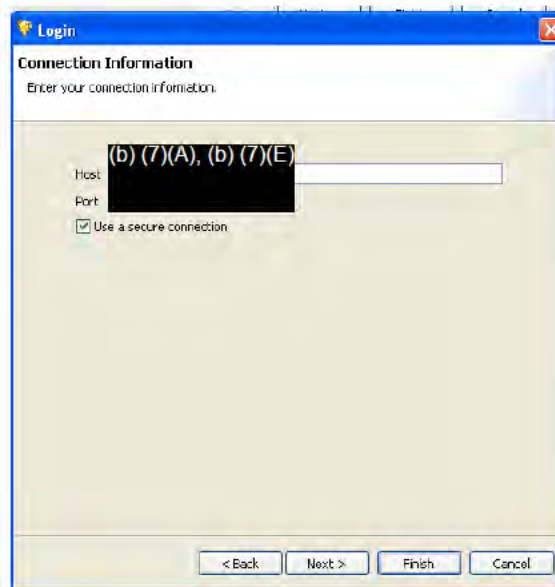
After the file is installed, analysts will need to adjust the programs configuration settings. When the login screen for the (b) (7)(E) comes up there a couple settings that need to be entered into the login screen to set up the connection. This information includes the domain you will be connecting to, your login credentials, and the port that will be used for the connection. Any variants in this information could result in a user having issues connecting to the necessary servers.

The initial login screen prompts the user for fairly basic information. This information includes a username, password, domain, and also asks if you want to use an existing account or create a new one. The ability to create a new account is not functional in this release of the (b) (7)(E) software, resulting in an error message when users attempt to do this. The rest of the information, with exception of resource is mandatory to successfully log into HSIN (b) (7)(E).

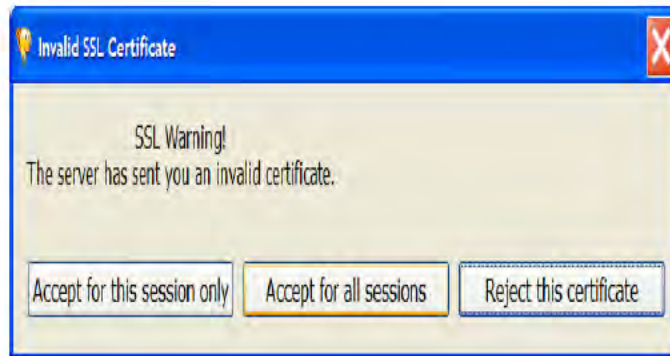
The username and password are specific to each individual user that is going to be logging into the client software. However, the domain information is going to be consistent for all users. The domain that needs to be supplied is "hsin.gov". Once this information has been entered it allows the user to save their password, this is not suggested for security reasons.



The second screen for the user login requires that the user enter the hostname which should be (b) (7)(A), (b) (7)(E) and the connection type to establish “select the checkbox that reads Use a secure connection”. Note, after entering (b) (7)(A), (b) (7)(E) and selecting the check box, the port number may change and you need to make sure you change it back to (b) (7)(A) again and then click next. These settings will remain consistent for all the users accessing (b) (7)(A), (b) (7)(E)



After clicking on next, the following screen will appear and you must select “Accept for all sessions”



11 Usernames, Passwords & Contact Information:

11.1 Passwords – See Internal Password Sheet

MMC Wifi Network:

(b) (7)(C), (b) (7)(E)
 [Redacted]

MMC Telephones:

(b) (7)(C), (b) (7)(E)
 [Redacted]

Desktops & Apple Mac Mini:

(b) (7)(C), (b) (7)(E)
 [Redacted] [Redacted] [Redacted]

Shared Drives:

(b) (7)(C), (b) (7)(E)
 [Redacted]

MMC DHS Email (Back Up)

(b) (7)(C), (b) (7)(E) (functions only in Microsoft Internet Explorer)

(b) (7)(C), (b) (7)(E)

Video Switch:

(b) (7)(C), (b) (7)(E)

Twitter/ Tweet Deck:

(b) (7)(C), (b) (7)(E)

11.2 NOC Contact Information

11.2.1 The SWO/KMO:

(b) (7)(A), (b) (7)(E), (b) (6)

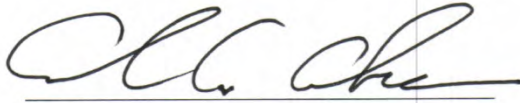
11.2.2 HSIN Help Desk:

(b) (7)(A), (b) (7)(E), (b) (6)

11.2.3 TSI Senior Reviewers:

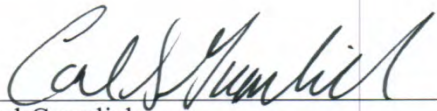
See MMC rosters in watch center

12 Responsible Official



Andrew Akers
Contracting Officer's Representative
Office of Operations Coordination and Planning
Department of Homeland Security

Approval Signature



Carl Gramlick
Director, National Operations Center
Office of Operations Coordination and Planning
Department of Homeland Security