# Analyst's Desktop Binder

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

2011

# Contents

1 Media Monitoring Capability Mission & Reporting Parameters: ..... 4
1.1 MMC Mission ..... 4
1.1.1 Leverage Operationally Relevant Data ..... 4
1.1.2 Support NOC in Identifying Relevant Operational Media ..... 4
1.1.3 Increase Situational Awareness of the DHS Secretary ..... 5
1.2 Critical Information Requirements ..... 5
1.3 Item of Interest Categorization ..... 5
1.4 Department of Homeland Security (DHS) Component Agencies ..... 7
1.5 DHS National Operations Center (NOC) Phases of Reporting ..... 8
1.5.1 NOC Notes ..... 8
1.5.2 Steady States ..... 8
1.5.3 National and International Situation Summary Updates ..... 8
1.5.4 Events of High Media Interest of International Significance ..... 9
1.5.5 NOC Numbered Items ..... 9
2 Items of Interest (IOI): ..... 10
2.1 Incidents that Warrant an IOI ..... 10
2.2 IOI Severity Chart ..... 10
2.3 Notification of MMC Management ..... 11
2.4 Critical Information Requirements ..... 12
2.5 IOI Categorization ..... 12
2.6 Credible Sources for Corroboration ..... 14
2.7 Sourcing IOIs ..... 15
2.8 IOI Distribution Lists ..... 15
2.9 Creating IOIs (Traditional Media Application) ..... 15
2.10 Creating IOIs (Social Media Application) ..... 17
2.11 Outlook Back-Up Procedure ..... 18
2.12 Correction Notices ..... 19
2.13 Key Words & Search Terms ..... 20
3 Personally Identifiable Information (PII) Guidance: ..... 24
3.1 Effective: January 7, 2011 ..... 25
4 Operational Summary Guidance: ..... 26

1.1.1. Operational Summary (OPSUM) Format: ..... 26
5 Retrieving NOC Priorities from Homeland Security Information Network (HSIN): ..... 29
1.1.2. NOC Priorities (HSIN Retrieval) ..... 29
6 Audio Video System: ..... 33
6.1 Direct TV Full Channel List ..... 33
6.2 Direct TV Account Information ..... 33
6.3 Online Audio-Video Switch ..... 33
7 HSIN(b) (7)(E) Connection Instructions: ..... 35
8 Usernames, Passwords & Contact Information: ..... 38
8.1 Passwords ..... 38
MMC Wifi Network: ..... 38
MMC Telephones: ..... 38
Desktops & Apple Mac Mini: ..... 38
Shared Drives: ..... 38
MMC DHS Email (Back Up) ..... 38
Video Switch: ..... 38
Twitter/ Tweet Deck: ..... 38
8.2 TSI Senior Reviewers ..... 39
The SWO/KMO: ..... 39
HSIN Help Desk: ..... 39
TSI Senior Reviewers: ..... 39

# 1 Media Monitoring Capability Mission & Reporting Parameters:

## 1.1 MMC Mission

The MMC has three primary missions:

- First - to continually update existing National Situation Summaries (NSS) and International Situation Summaries (ISS) with the most recent, relevant, and actionable open source media information
- Second - to constantly monitor all available open source information with the goal of expeditiously alerting the NOC Watch Team and other key Department personnel of emergent situations
- Third - to receive, process, and distribute media captured by DHS Situational Awareness Teams (DSAT) or other streaming media available to the NOC such as Northern Command's (NORTHCOM) Full Motion Video (FMV) and via open sources

These three missions are accomplished by employing various tools, services, and procedures that are described in detail in this document. Expanded upon, these primary missions have three key components:

### 1.1.1 Leverage Operationally Relevant Data

Leveraging news stories, media reports and postings on social media sites 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 every direction and interest, utilizing thousands of reporters, sources, still/video cameramen, analysts, bloggers and ordinary individuals on scene. Traditional Media outlets provide unmatched insight into the depth and breadth of the situation, worsening issues, 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 works to summarize the extensive information from these resources to provide a well rounded operational picture for the Department of Homeland Security.

### 1.1.2 Support NOC in Identifying Relevant Operational Media

Supporting the NOC by ensuring they have a timely appreciation for 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 other evolving situations in that area. These situations may be related; have a cause and effect relationship; or be unrelated but have a detrimental effect. Through coordination with the NOC Duty Director (NDD), 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.

Timely reporting of current information is an integral element in maintaining complete operational awareness by Homeland Security Personnel. The MMC understand it is vital that

critical information is relayed to key Department decision makers in as expeditious a manner as possible.

#### 1.1.3 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 monitors news coverage with the perspective of how the breaking story may be related to current and other important ongoing situations and DHS activities.

The on-duty MMC analyst alerts DHS personnel and related federal agencies of updated news stories through distributed Items of Interest (*see section 3.9.6*). Recognizing that local media coverage is potentially sensationalizing an incident, the MMC strives to comprehend the media's message and identify sensitive situations that must be brought to the attention of the Secretary.

## 1.2 Critical Information Requirements

The attribution of IOIs by CIR allows the MMC to catalog articles into five specific categories depending on the potential impact or type of article that is being distributed. These CIRs include:

1) Potential Threat to DHS, other federal, and state/ local response units, facilities, and resources.
2) Potential impact on DHS capability to accomplish the HSPD-5 mission
3) Identifying events with operational value…corroborating critical information
4) Identifying media reports that reflect adversely on DHS and response activities
5) Standing HSC planning scenarios

## 1.3 Item of Interest Categorization

The categorization of IOIs in the daily log allows analysts to track the types of articles that are distributed as they relate to 14 characterizations. These 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.

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, reports on 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 with regard to immigration in the United States, and border control issues.
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 and response to suspicious powder and chemical or biological agents.
7) **Nuclear**: To include 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**: To include reports on security breaches, airport procedures, and other transportation related issues, and any of the above issues that affect transportation. Reports will include threats toward and incidents involving rail, air, road, and water transit in the United States.
9) **Infrastructure**: 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, as well as those listed above.
10) **National/International Security**: Includes reports on threats or actions taken against United States national interests both at home and abroad. Reports would include articles related to threats against American citizens, political figures, military installations, embassies, 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 articles 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) **Reports on DHS, Components, and other Federal Agencies**: Includes both positive and negative reports on FEMA, CIS, CBP, ICE, etc. as well as organizations outside of DHS.
14) **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 strategies and tools that aid or affect communications and management of crises.

## 1.4 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, and 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.

## 1.5 DHS National Operations Center (NOC) Phases of Reporting

### 1.5.1 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 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 a Steady State or become resolved rather quickly. These do not get added to the COP (only NSSs/ISSs), but the MMC will continue to publish IOIs on the event until the NOC determines that the situation has been resolved.

### 1.5.2 Steady States

Steady States are IOI's that have a higher precedence over general IOIs or NOC Notes (many Steady States are produced as a result of a NOC Note), but are not quite as relevant as NSSs or ISSs. Each of these covers a singular event continuously and could upgrade to an NSS or ISS item over a period of time depending on the situation. These do not get added to the COP, but the NOC and the MMC will continue to monitor such IOIs until the event has been resolved.

### 1.5.3 National and International Situation Summary Updates

Distributed National Situation Summary (NSS) Updates or International Situation Summary (ISS) updates are formatted in the same manner as all other types of IOIs, but are utilized to provide supplemental information for COP updates to active NSS/ISSs. These reports provide

the NOC Watch Team with a summary of media reports on a particular NSS/ISS and to increase the overall situational awareness of the NOC. The NSS/ISS updates include a brief synopsis of the incident's latest developments, an overview of broadcast television media coverage, and a summary of print news media coverage.

For loading NSS/ISS updates to the COP, please refer to COP posting information beginning in Section 4.1.2, Media Monitoring User Page. Figure 7 is an example of the format for NSS/ISS updates.

### 1.5.4 Events of High Media Interest of 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 (Section 3.9.23, National Operations Center 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 seem to be a high priority for the NOC, and in this case, would simply be used to enhance situational awareness. Some of these events may be issued an NOC-assigned number and in this case, the MMC will publish IOIs in the same manner as it would for NOC Notes, Steady States, or NSSs/ISSs. These do not get added to the COP unless the NOC directs the MMC to do so.

### 1.5.5 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, Steady State 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 #0012-11: Suspicious Activity – Chemical, Biological, Radiological, Nuclear or Explosive (CBRNE)**: covering any suspicious incident which may involve a CBRNE or CBRNE threat.
- **NOC #0013-11: Suspicious Activity**: Covers any suspicious incident which does not involve a CBRNE
- **NOC #0014-11: Public Safety/Unusual Activity**: Covers any incident that is not suspicious in nature, but needs further information or tracking

**Example:** NOC 0012-11-295 [Suspicious Powder, Anchorage, AK]

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

# 2 Items of Interest (IOI):

MMC coverage focuses primarily on providing information on incidents of national significance, 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.

**Note -** Reports that pertain to DHS and sub agencies - especially those that have a negative spin on DHS/Component preparation, planning, and response activities should be reported to management before being sent to the distribution list. Senior TSI personnel will decide whether the information should be reported through normal channels. If there are ANY questions about whether an incident or other reported item is a valid IOI article check with management.

## 2.1 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 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, debates, and implementations related to DHS

## 2.2 IOI Severity Chart

The Item of Interest (IOI) Severity Chart is a tool that provides MMC analysts with a process to assess the severity of a news story and the urgency in which the corresponding IOI should be distributed. Determining the severity of an IOI allows analysts to triage news stories and send out time-sensitive pieces first, followed by less acute stories. The IOI Severity Chart is broken down into five categories, from "Urgent" to "Validate." Each category explains the threat assessment, when distribution should occur, and the probable source. So, for example, if an analyst has two stories that are fit to distribute, the analyst will use the Severity Chart to determine the order of distribution and follow-ups. Let's say the analyst has one story on an explosion at a subway stop in New York City and another story on a policy change to passport purchases. According to the IOI Severity Chart, the explosion falls into Category 2, "Critical," and requires immediate distribution. The change in passport purchase policy falls into Category 4, "Routine," and has a more lax distribution protocol. In this instance, the analyst would immediate distribute the story on the explosion at a subway stop in New York City. Only after

additional follow-ups on the outcome and cause of the explosion would the second article on passport policy be distributed.

| Category | Threat Assessment | Distribution | Probable Source |
|---|---|---|---|
| 1 – Urgent | **Catastrophic:** Bombing with casualties (excluding Afghanistan and Iraq), tsunami, mass shootings, terrorist attack, train derailment with mass causalities, major attack and/or destruction of U.S. infrastructure. | Immediate | Breaking news on National Broadcast (Fox News, CNN, etc.). Foreign and Regional press (BBC, Sky News, etc.) Story has not yet reached national or local print. |
| 2 – Critical | **Highly destructive/poses a threat to a large group of people and/or resources:** HAZMAT situation, tornado, hurricane, wildfires, mass flooding, publicized terrorist threat, suspicious package and/or substance, harm (accidental or intentional) to a large group of people and/or resources. | Immediate | Breaking news on National Broadcast (Fox News, CNN, etc.) and national and/or local print. |
| 3 – Priority | **Low threat to a specific area, potential for incident to upgrade to Category 1 and/or 2:**<br><br>Border patrol incidents (with violence), severe weather, health concerns/recalls, train derailment, chemical spill, etc. | After Category 1 and 2 stories and follow-ups have been released by MMC.<br><br>The story has been reviewed for timeliness and accuracy. | National and/or local print, UK news (BBC, Sky News). |
| 4 – Routine | **Of Interest:**<br><br>Border incidents (with no violence), drug busts, localized crime and/or related incidents, immigration, additional articles that are not subjective in nature. | When there is a significant lull in MMC releases and after the story has been verified from several sources. | National and/or local print, Western European and Canadian news sources. |
| 5 – Validate | **Subjective:**<br><br>Reports on federal agencies, (particularly as related to DHS activity), research/ studies, etc. | Upon verification from Brad, Mitch, Ray, or one of the team leads. | Local print, medical reviews, foreign news agencies (with the exception of Western Europe and Canada). |

It is important to note that although the IOI Severity Chart provides guidance in determining the category of a potential IOI, there will be times when a story fails to fall into a specific category. When in doubt of whether an article should be distributed, it is the analyst's responsibility to contact one of the managers or team leads to receive direction and confirmation on handling the IOI in question.

## 2.3 Notification of MMC Management

TSI management is an integral part of MMC operations are to be used to augment understanding and proficiency of MMC policies and procedures. When there is ever a question that cannot be answered through the SOP or the analyst's own deductive reasoning, then the analyst must call TSI management to receive proper guidance. Times when you must call Brad, Mitch or Ray (or others when directed) are when:

- Something significant has occurred
- A particular report seems IOI worthy, but there are no corroborating reports

- The initial IOI worthy report and the corroborating report are not from the source list we typically use
- The IOI worthy report reflects negatively on DHS or some other federal agency
- It appears the IOI worthy report will require numerous updates and potentially be an enduring topic
- You are not sure if an event has already been reported during a previous watch
- You feel a correction must be issued
- You are experiencing system problems – even if you have addressed them
- Whenever you have had to employ your backup
- You are simply not sure about a particular report and want a second opinion
- You have been given special instructions from DHS-related personnel such as the NOC SWO

## 2.4 Critical Information Requirements

The attribution of IOIs by CIR allows the MMC to catalog articles into five specific categories depending on the potential impact or type of article that is being distributed. These CIRs include:

1) Potential Threat to DHS, other federal, and state/ local response units, facilities, and resources.
2) Potential impact on DHS capability to accomplish the HSPD-5 mission
3) Identifying events with operational value…corroborating critical information
4) Identifying media reports that reflect adversely on DHS and response activities
5) Standing HSC planning scenarios

## 2.5 IOI Categorization

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.

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, reports on 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 with regard to immigration in the United States, and border control issues.
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 and response to suspicious powder and chemical or biological agents.
7) **Nuclear**: To include 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**: To include reports on security breaches, airport procedures, and other transportation related issues, and any of the above issues that affect transportation. Reports will include threats toward and incidents involving rail, air, road, and water transit in the United States.
9) **Infrastructure**: 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, as well as those listed above.
10) **National/International Security**: Includes reports on threats or actions taken against United States national interests both at home and abroad. Reports would include articles related to threats against American citizens, political figures, military installations, embassies, 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 articles 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) **Reports on DHS, Components, and other Federal Agencies**: Includes both positive and negative reports on FEMA, CIS, CBP, ICE, etc. as well as organizations outside of DHS.
14) **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 strategies and tools that aid or affect communications and management of crises.

## 2.6 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 d*o 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),

**Second Tier -** *Should ideally 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
  - MoveOn.org, Amnesty International, etc.

**Third Tier –** *Must be verified by a First Tier source prior to release.*

- 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.

**Fourth Tier –** *Must be verified by a First Tier source prior to release*

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

## 2.7 Sourcing IOIs

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

## 2.8 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 listing of the different lists and the purpose of each. *In rare cases, one or more lists will be allowed for use.*

1) **Default –** this is a full distribution (FULLDIS) list that (more than just NOC personnel listed) 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 to certain DHS, NOC, and TSI Leadership. IOIs that are sent utilizing the LIMDIS list are major traffic disruptions, suspicious package/powder incidents, hazmat, and school lockdowns.

3) **SN-Only** – this is reserved for the SN team and includes specific members of the DHS Privacy office.

4) **SPECDIS** – also known as Special Distribution List, is determined by Management and is used in rare cases, unusual events, or for certain individuals.

5) **TSI Test** – used for training and test purposes.

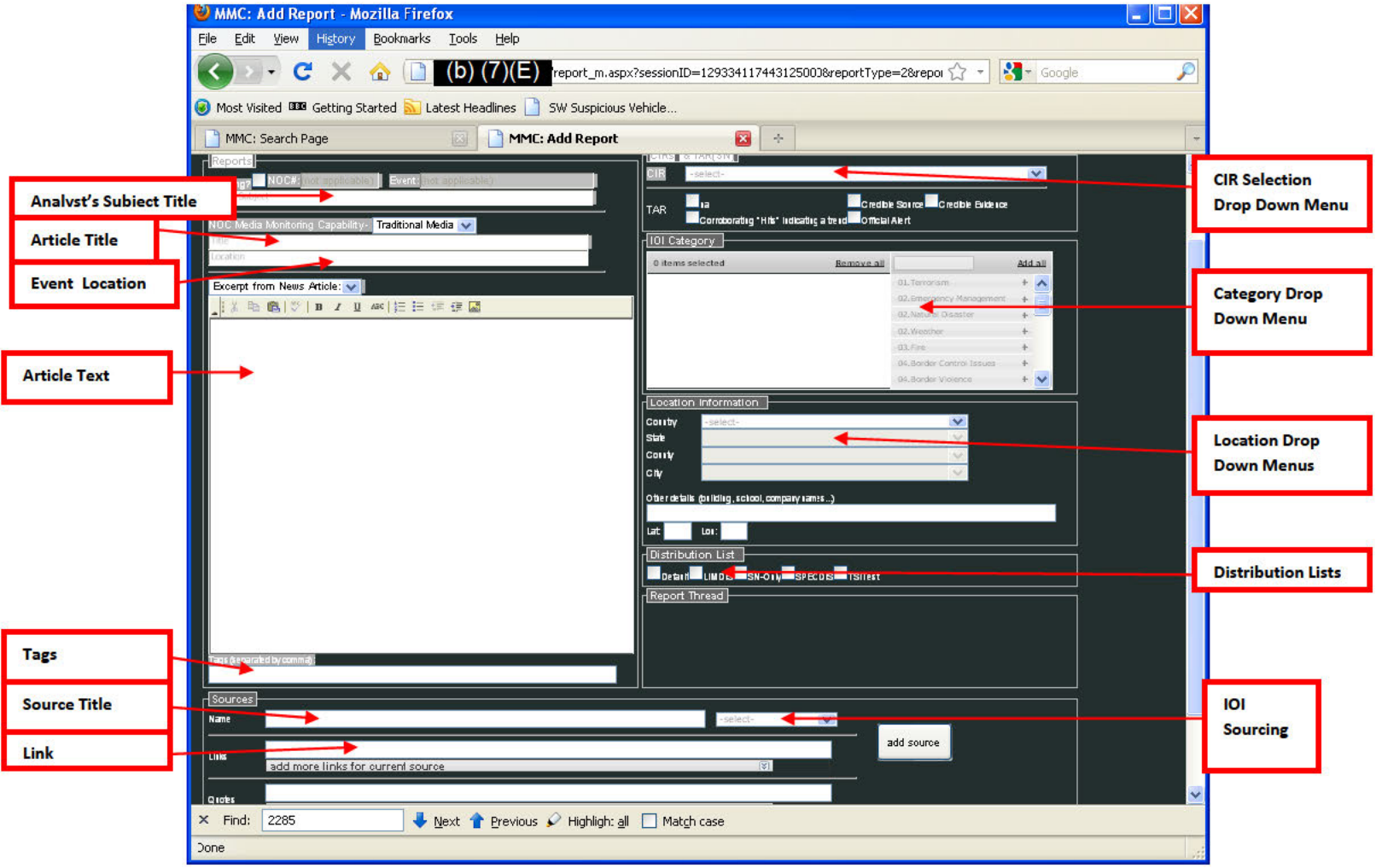
**Note:** For a current copy of any of the above IOI distribution lists, please refer to management and request that distribution list be sent to you.

## 2.9 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 CIR# from the drop down menu.
- 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, SN Only)
- Proofing the entire report
- Verifying that the format is correct

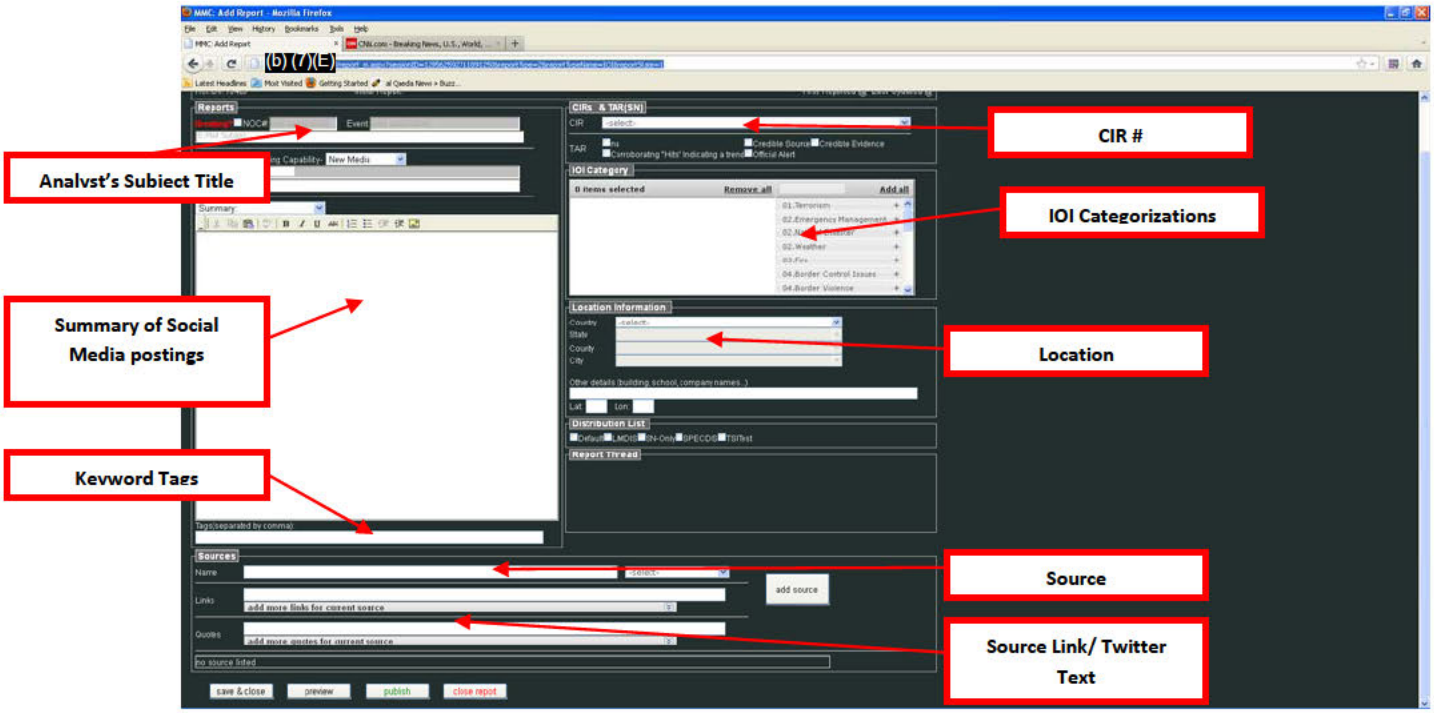


## 2.10 Creating IOIs (Social Media Application)

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:

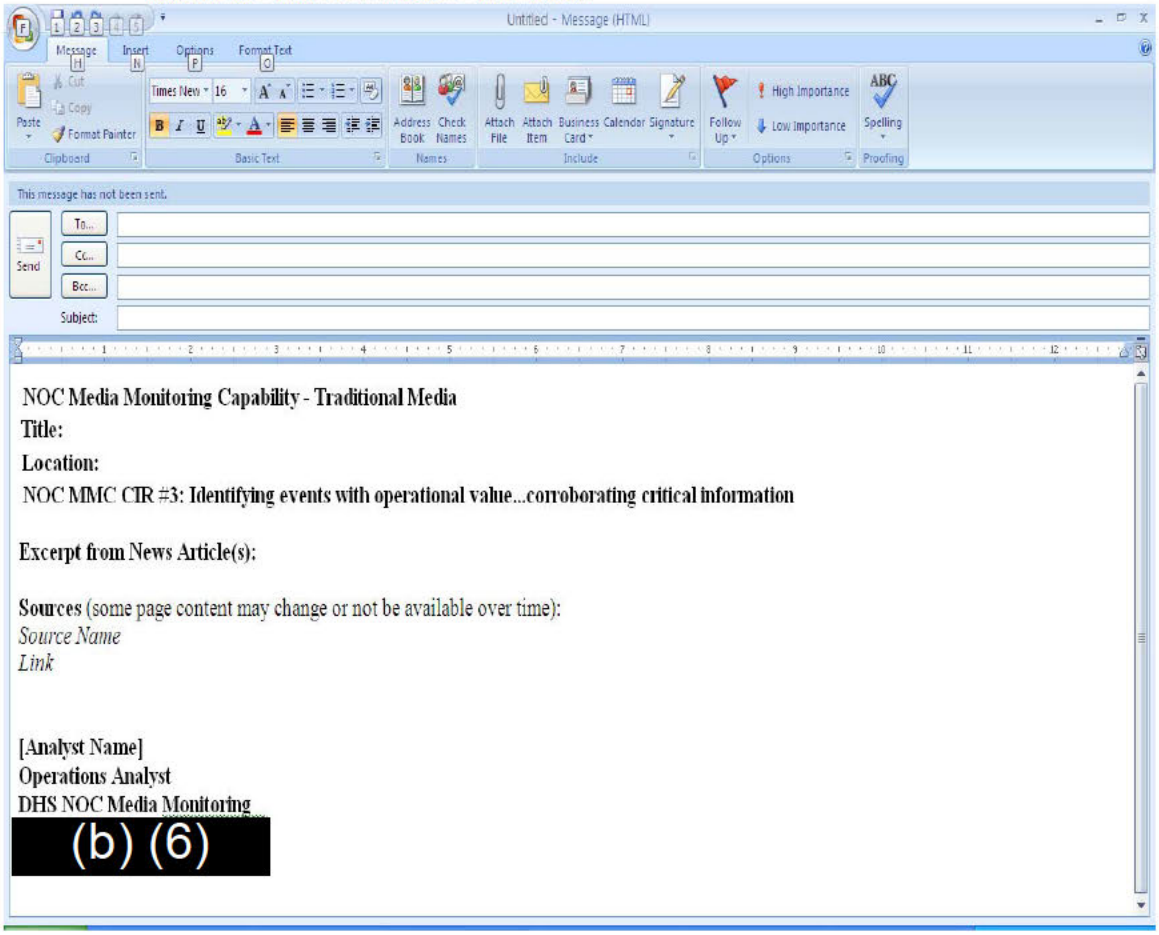
- Generating a subject line that summarizes the main points of the article in a clear and concise manner and entering it in the proper field.
- Selecting the correlating CIR# from the drop down menu.
- Selecting the most specific location possible from the drop down menu.
- Pulling relevant points from 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 correct distribution list (Default, Limdis, Specdis, SN Only)
- Proofing the entire report
- Verifying that the format is correct



## 2.11 Outlook Back-Up Procedure

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
- Copy and paste the title of the article into the Title line and 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.
- Select the CIR # that best corresponds to the incident.
- Insert the article's text.
- Insert the article's source and link.



## 2.12 Correction Notices

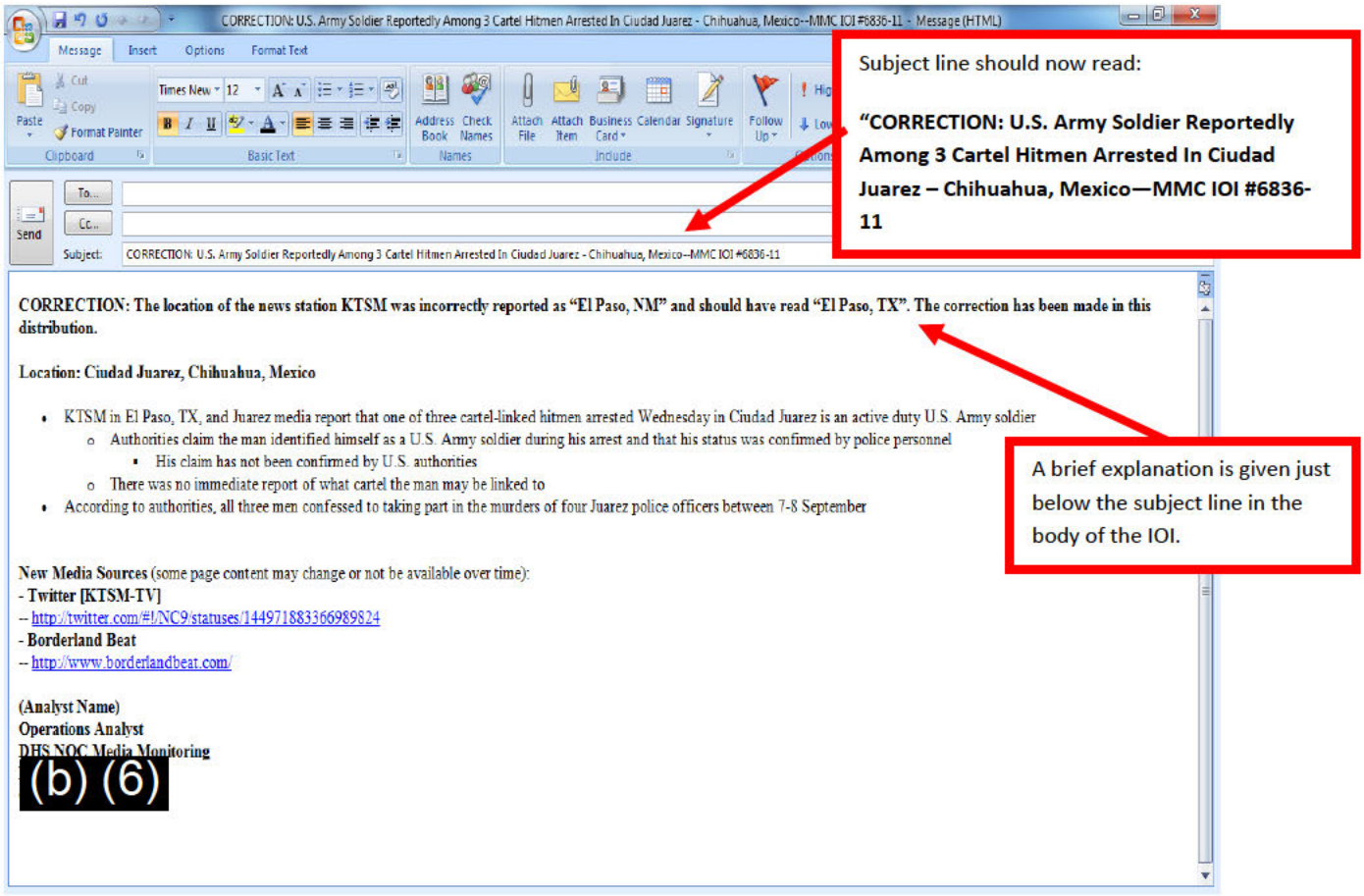
Correction notices are issued in the event incorrect information is distributed in an IOI. The magnitude of misinformation can range from a misspelled word to a missing link. Whenever the analyst finds a mistake in a distribution after the item is sent, the first step the analyst will take is to contact management and inform management 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: U.S. Army Soldier Reportedly Among 3 Cartel Hitmen Arrested In Ciudad Juarez – Chihuahua, Mexico—MMC IOI #6836-11**

*Sample Correction Summary:* **CORRECTION: The location of the news station KTSM was incorrectly reported as "El Paso, NM" and should have read "El Paso, TX". The correction has been made in this distribution.**




## 2.13 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. The new search terms will not use PII in searching for relevant mission-related information

**DHS & Other Agencies**

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

**Domestic Security**

Assassination
Attack
Domestic security
Drill
Exercise
Cops
Law enforcement
Authorities
Disaster assistance
Disaster management
DNDO (Domestic Nuclear Detection Office)
National preparedness
Mitigation
Prevention
Response
Recovery
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
Torreon
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)
ETA (Euskadi ta Askatasuna)
Basque Separatists
Hezbollah
Tamil Tigers
PLF (Palestine Liberation Front)
PLO (Palestine Liberation Organization
Car bomb
Jihad
Taliban
Weapons cache
Suicide bomber
Suicide attack
Suspicious substance
AQAP (AL Qaeda Arabian Peninsula)
AQIM (Al Qaeda in the Islamic Maghreb)
TTP (Tehrik-i-Taliban Pakistan)
Yemen
Pirates
Extremism
Somalia
Nigeria
Radicals
Al-Shabaab
Home grown
Plot
Nationalist
Recruitment
Fundamentalism
Islamist

**Weather/Disaster/Emergency**

Emergency
Hurricane
Tornado
Twister
Tsunami
Earthquake
Tremor
Flood
Storm
Crest
Temblor
Extreme weather
Forest fire
Brush fire
Ice
Stranded/Stuck
Help
Hail
Wildfire
Tsunami Warning Center
Magnitude
Avalanche
Typhoon
Shelter-in-place
Disaster
Snow
Blizzard
Sleet
Mud slide or Mudslide
Erosion
Power outage
Brown out
Warning
Watch
Lightening
Aid
Relief
Closure
Interstate
Burst
Emergency Broadcast System

**Cyber Security**

Cyber security
Botnet
DDOS (dedicated denial of service)
Denial of service
Malware
Virus
Trojan
Keylogger
Cyber Command
2600
Spammer
Phishing
Rootkit
Phreaking
Cain and abel
Brute forcing
Mysql injection
Cyber attack
Cyber terror
Hacker
China
Conficker
Worm
Scammers
Social media

# 3 Personally Identifiable Information (PII) Guidance:

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 sending out ANY reports, including IOIs, ]\al33l analysts must ensure that if there is any PII included in a media article, that information must be removed, due to privacy issues! (*Figure 6, IOI Example* )

Generally, both MMC and SN must never send out any IOIs with PII included except in "extremis situations". An extremis situation occurs when there is 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, TSI management would need to be made aware of the situation). ***Note:*** *The DHS OPS authority includes OPS Senior Executive leadership and the SWO.*

The following are cases in which PII must be removed from all MMC reports:

**1)** Names, positions, or other information that would enable someone to determine the identity of a particular person
   a. The Privacy Impact Assessment (PIA) allows for certain exemptions in which PII may be included to identify spokesmen, government officials and reporters. ***Note:*** *Refer to section 3.1 and the current PIA for more information*

***2)*** Names of known or suspected terrorists, DTO leaders, or other individuals who are a threat to homeland security, regardless of whether a U.S. citizen or non-U.S. citizen

**3)** Links to the actual articles or postings referenced provided the links themselves do not contain PII. In this case the analyst would use "No Link Due To PII" instead of the actual link.

**4)** Addresses that would reveal where a person lives. In this case the analyst would either delete the street address completely generalize it to the street block. Example: instead of using "1345 John Doe Avenue", the analyst could use "the 1300 block of John Doe Avenue".

**Note:** The MMC watch may provide the name, position, or other information considered to be PII to the NOC over the telephone when approved by the appropriate DHS OPS authority. But that information must not be stored in a database that could be searched by an individual's PII.

### 3.1 Effective: January 7, 2011

OPS conducted an update to the Privacy Impact Assessment (PIA) allowing the Media Monitoring Capability to now collect and disseminate PII for certain narrowly tailored categories. Furthermore, PII on the following categories of individuals may be collected when it lends credibility to the report or facilitates coordination with federal, state, local, tribal, territorial, foreign, or international government partners:

*1)* U.S. and foreign individuals *in extremis* situations involving potential life or death circumstances; *(this is no change)*
*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.

**NOTE**: PII on these individuals may include: 1) full name; 2) affiliation; 3) position or title; and 3) publicly-available user ID. Analysts are trained to use only approved PII that is easily identifiable and to ignore and exclude any non-authorized PII. *Practical implementation: the PII must add value, i.e. we can now say Sheriff or Fire Chief, but if the name is not important (and it usually isn't) don't include the name, just the title, especially for lower level officials.* Should PII come into the NOC's possession, apart from these categories, the NOC shall redact it prior to further dissemination of any collected information. (Current PII retraction procedures do not change)

**What was NOT Approved:**
- We **will not report** on Individuals suspected or accused of committing crimes of National or Homeland Security interest, if captured, (see # 7 above for the exception if they are killed or found dead)
- We **will not report** on Private citizens no matter if they are witnesses, victims, observers or some other way connected to an event
- We **will not report** on high profile people such as celebrities, sports figures or media members who are victims. (see # 6 above for the exception if they are current or former public officials)

# 4 Operational Summary Guidance:

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 highly coordinated with TSI senior management before distribution.

Both the on duty Traditional and Social Media Analysts will collaborate to generate a single report and then submit it to the designated TSI Senior Reviewer no later than 0400. The Senior Reviewer will check the report for proper grammar, punctuation, 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:
  - (b) (6) n the TO Line
  - (b) (6) (b) (6) (b) (6) in the BCC Line
- The OPSUM must not be distributed any earlier than 0445, 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 in responsible for notifying the TSI Senior Reviewer for that shift as soon as possible that the time production time has been adjusted.

## 4.1 Operational Summary (OPSUM) Format:

Operational Summaries (OPSUM) are distributed each morning to provide recipients with the most current statistics for ongoing situations (e.g. NSS/ISSs, Steady-States), and events of high media interest. As such, the OPSUM format directly reflects the published NOC Priorities. Analyst will gather the most current media information on the active situation(s) 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
- Analyst 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.

- Sources will be included with the bullets for items of high interest or particularly controversial summaries. SN analysts will include links to translated articles if using foreign language sources.

**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 Violence
- **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))**
  - Commercial Aviation Cargo Threats/Incidents in the U.S. and Overseas
  - Indications of Mass Migration in the Caribbean
  - CBRNE Threats/Incidents in the U.S. and its Territories

Hyper Links Take Reader To Relevant Sections

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

**NOC 0003-11: Southwest Border Violence - U.S./Mexico Border**

**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, Guerrara, after the arrest of one of his bosses, unleashing a wave of executions of rival group members

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

Sources Included for Bullets Including Significant Value or Controversial Information

***Killings (non U.S. persons)*** *(Social Media)*

- *Three separate grenade attacks in Mexican cities over the weekend have resulted in 1 death and 7 injuries 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*
- *The director of the Ixtlahuacán del Río Police was executed on Saturday night in an ambulance in the municipality of Cuquio 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*
  - *The murderers beat emergency medical technicians after the execution and fled*

***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 there are up to 500 gangs in the area ranging between 5,000 and 7,000 members.

[Back to top]

**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*
- *Duke Energy reports 1,516 outages remaining across 5 Indiana counties*

Double Space Between Sections

**New Al Qaeda Leader Urges Attacks on the U.S.** Fox News (AP)

- In a video posted on militant websites Sunday, Al Qaeda's new leader called on followers to avenge the killing of Osama bin Laden and to continue the Islamist jihad against America
  - The leader also stated that uprisings in Egypt and Tunisia have presented Al Qaeda with opportunities to spread its message throughout the Arab world
  - Al Qaeda has tried to forge a role for itself in the recent uprisings though it has little in common with the mainly youth activists behind the protests…. most uprising leaders say they seek greater freedoms, not Islamic states

**Continued Violence in Syria** Reuters

- Syrian forces shelled residential districts in Latakia on Monday, the third day of an assault on Sunni neighborhoods of the port city
  - *Approximately 35 people, and possibly more, have been killed in the city since the assault on Latakia began on Saturday, activists and witnesses say (Social Media)*
- *More than 5,000 Palestinian refugees have fled a camp in Latakia (Social Media)*
  - *It was not immediately clear where the refugees were seeking shelter (Social Media)*
  - *A UN spokesman reports that "there were 10,000 refugees in the camp" prior to the attack (Social Media)*
- Separately, troops conducted raids and arrests in the village of Houla
- *UN authorities cite reports that Syrian security forces have opened fire on defectors within their own ranks and executed troops that refused orders to kill civilians (Social Media)*
  - *"There are indications that more than 300 security forces or army personnel have died, in circumstances that remain to be elucidated, but could include clashes with armed opposition as well as internal executions of defecting soldiers," officials said (Social Media)*

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

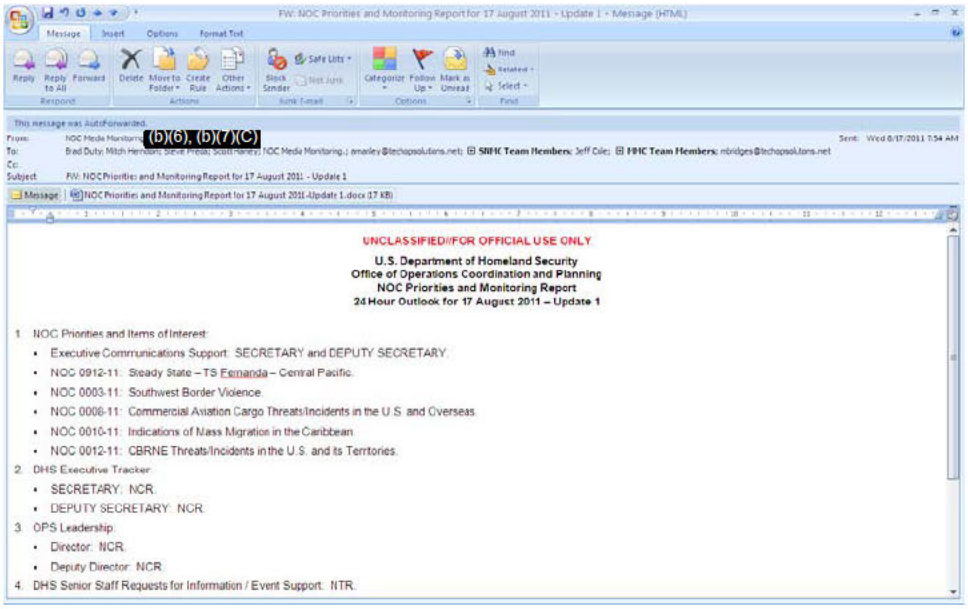
[Back to top]

Link takes reader back to top of report

**Analyst's Name**
**Operations Analyst**
**DHS NOC Media Monitoring**
**Phon**
**Cell:** (b) (6)

# 5 Retrieving NOC Priorities from Homeland Security Information Network (HSIN):

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.



FW: NOC Priorities and Monitoring Report for 17 August 2011 - Update 1 - Message (HTML)

Message | Insert | Options | Format Text

Reply | Reply to All | Forward | Delete | Move to Folder | Create Rule | Other Actions | Block Sender | Safe Lists | Not Junk | Categorize | Follow Up | Mark as Unread | Find | Related | Select

This message was AutoForwarded.

From: NOC Media Monitoring (b)(6), (b)(7)(C)

To: Brad Duty; Mitch Herndon; Steve Preiss; Scott Haney; NOC Media Monitoring.; smarley@techopsolutions.net; SMHC Team Members: Jeff Cole; HHC Team Members: mbridges@techopsolutions.net

Cc:

Subject: FW: NOC Priorities and Monitoring Report for 17 August 2011 - Update 1

Sent: Wed 8/17/2011 7:54 AM

Message | NOC Priorities and Monitoring Report for 17 August 2011-Update 1.docx (17 KB)

UNCLASSIFIED//FOR OFFICIAL USE ONLY

**U.S. Department of Homeland Security**
**Office of Operations Coordination and Planning**
**NOC Priorities and Monitoring Report**
**24 Hour Outlook for 17 August 2011 – Update 1**

1. NOC Priorities and Items of Interest:
   - Executive Communications Support: SECRETARY and DEPUTY SECRETARY.
   - NOC 0912-11: Steady State – TS Fernanda – Central Pacific.
   - NOC 0003-11: Southwest Border Violence.
   - NOC 0008-11: Commercial Aviation Cargo Threats/Incidents in the U.S. and Overseas.
   - NOC 0010-11: Indications of Mass Migration in the Caribbean.
   - NOC 0012-11: CBRNE Threats/Incidents in the U.S. and its Territories.
2. DHS Executive Tracker:
   - SECRETARY: NCR.
   - DEPUTY SECRETARY: NCR.
3. OPS Leadership:
   - Director: NCR.
   - Deputy Director: NCR.
4. DHS Senior Staff Requests for Information / Event Support: NTR.

## 5.1 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

HSIN Government Portal
Home

Your Contact Card

Organization: TECH OP Solutions International
First Name: Michael
Middle Initial:
Last Name: (b)(6), (b)(7)(C)
Email Address:
Mobile Email Address:
Title: Operations Center Media Analyst
Address Name: (b)(6), (b)(7)(C)
Address Line 1:
Address Line 2:
City: Washington D.C.
County:
State: Washington, D.C.
Postal Code: 20016
Country: United States
First Choice of Contact: EmailAddress
Second Choice of Contact: Business Phone
Third Choice of Contact:

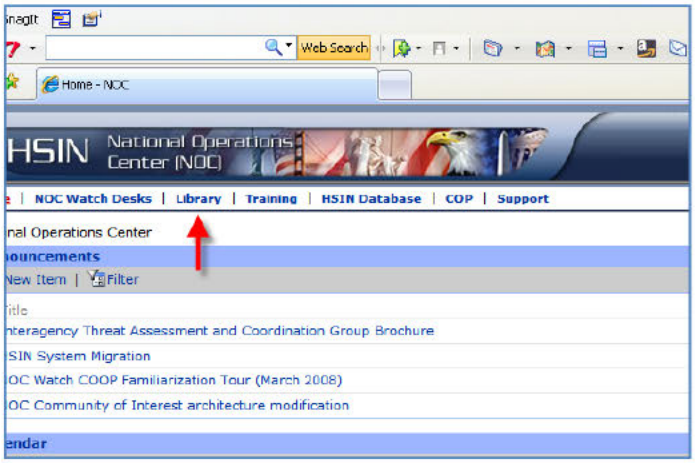
Your Address Book
Edit Your Information
Change Your Password
View Community List

Business Phone: (b)(6), (b)(7)(C)
Mobile Phone:
Pager:
Other Phone:

Your Communities
Federal
Emergency Management
Federal Operations
HSIN Government Home
National Operations Center

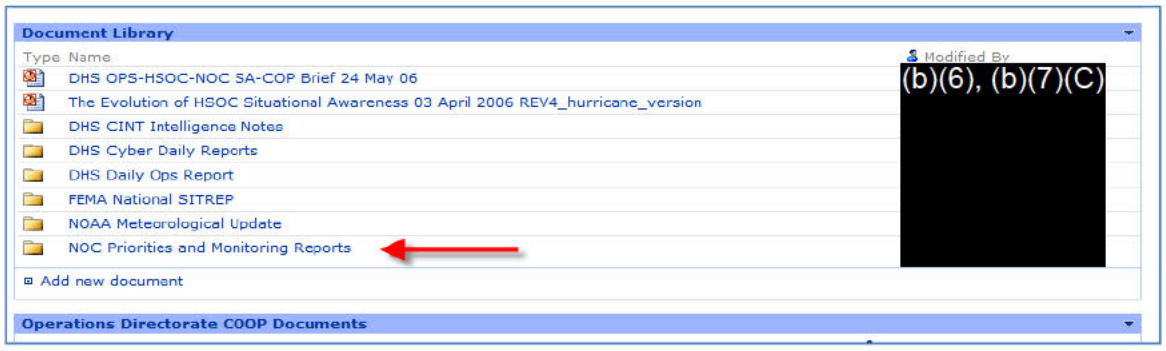
2) **Step Two:** Select the **National Operations Center Tab** in the lower left corner.


3) **Step Three:** Select the **Library Tab**.



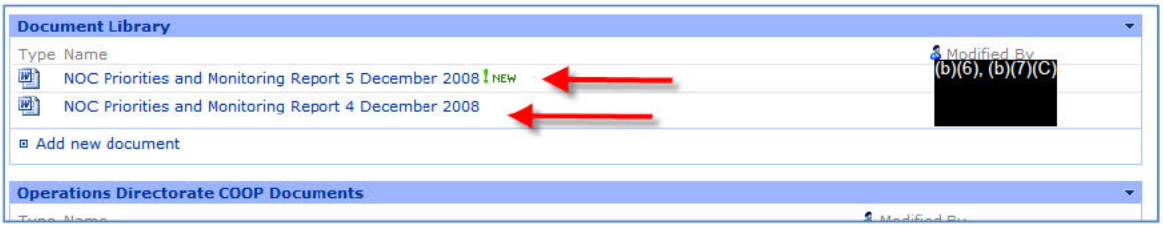

4) **Step Four:** Scroll down to the **document library section**.


5) **Step Five:** Select the **NOC Priorities** folder:



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


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



# 6 Audio Video System:

## 6.1 Direct TV Full Channel List

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

## 6.2 Direct TV Account Information

Contact (b)(6), (b)(7)(C)

## 6.3 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: http: (b) (7)(E)

**Username:** (b) (7)(E)
**Password:** (b)(7)(E) (There is one universal username/password for everyone)

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).

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

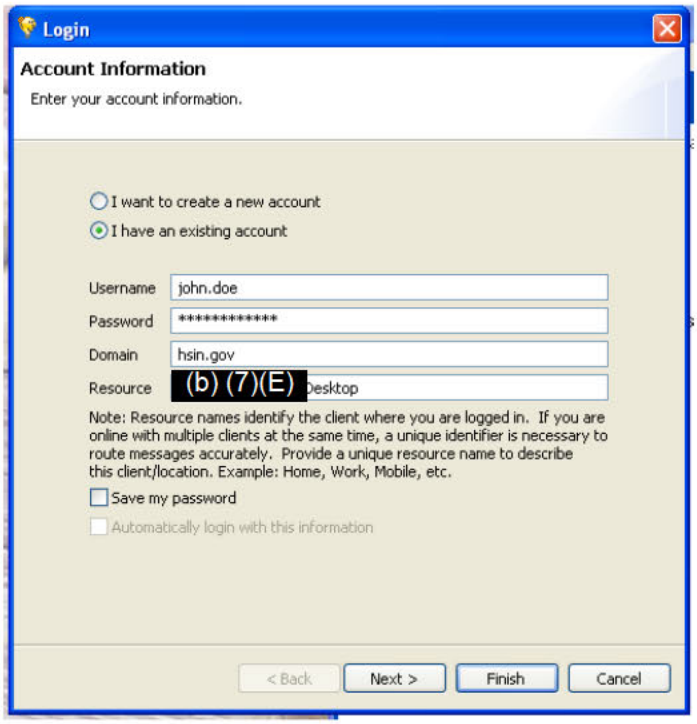
(b) (7)(E) is a text based communications tool utilized by the Department of Homeland Security to connect individuals at different locations. The MMC utilizes (b) (7)(E) as a means to communicate with members of the NOC Watch throughout the shift. The NOC has a dedicated chat room, identified as NOC_Watch 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.

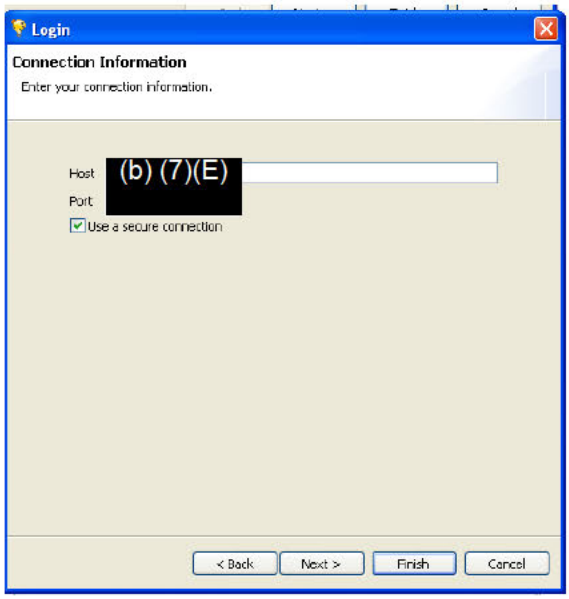
After the file is installed, analysts will need to adjust the programs configuration settings. When the login screen for the (b) (7)(E) thick client comes up there a couple settings that need to be entered into the login screen to set up the connection. This information includes the domain you will be 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) thick client 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)

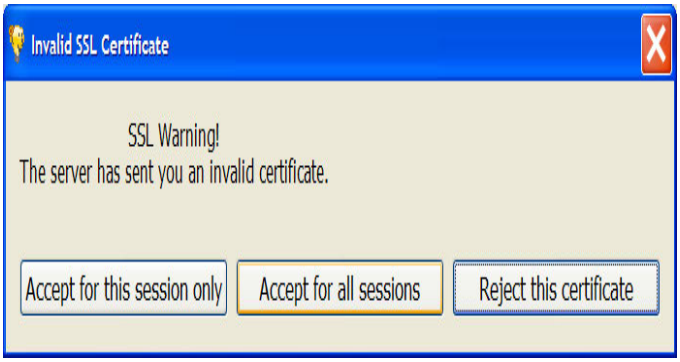
The username and password are specific to each individual user that is going to be logging into the client software. However, the domain information is going to consistent for all users. The domain that needs to be supplied is "hsin.gov". Once this information has been entered it allows the user to save 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)(E), the port which should be (b) (7)(E) and the connection type to establish "select the checkbox that reads Use a secure connection". Note, after entering port 443 and selecting the check box, the port number may change and you need to make sure you change it back to (b) (7)(E) again and then click next. These settings will remain consistent for all the users accessing HSIN (b) (7)(E)



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



# 8 Usernames, Passwords & Contact Information:

## 8.1 Passwords

**MMC Wifi Network:**

Network Name: MMC –SN
Password (b) (7)(E)
Network Name: MMC –SN (BackUp)
Password: (b) (7)(E)

**MMC Telephones:**

MMC Office Voicemail (b) (6)
SN Office Voicemail: (b) (6)
Blast Call Cell Phone: (b) (6)

**Desktops & Apple Mac Mini:**

| | | |
|---|---|---|
| MMC Desktop: | U: MMC Analyst | P: (b) (7)(E) |
| MMC Mac: | U: MMC Analyst | P: |
| SNMC Mac: | U: snmc analyst | P: |
| MMC Outlook | U: (b) (6) | P: |
| Meltwater | U: | P: |

**Shared Drives:**

MMC Address (b) (7)(E)
SN Address: (b) (7)(E)
Username: (b) (7)(E)
Password:

**MMC DHS Email (Back Up)**

https://connect.dhs.gov (functions only in Microsoft Internet Explorer)
Username: (b) (6)
Password (b) (7)(E) (changes every 90 days)
Password Reset: (b) (6)

**Video Switch:**

Address: (b) (7)(E)
Click "VIDEO SWITCH"
Username: (b) (7)(E)
Password:

**Twitter/ Tweet Deck:**

Twitter:
Username: DHSNOCMMC1
Password: (b) (7)(E)
TweetDeck
Email: (b) (6)
Password: (b) (7)(E)

## 8.2 TSI Senior Reviewers

**The SWO/KMO:**

(b) (6)

(b)(6), (b)(7)(E) room: NOC_Watch

**HSIN Help Desk:**

**HSIN Help Desk:** (b)(6)
(b) (6)

**NOC HSIN Desk:** (b) (6)
(b) (6)

**TSI Senior Reviewers:**

(b)(6), (b)(7)(C)