INTERAGENCY INTEGRATED SOP APPENDIXES AND ANNEXES

JOINT FIELD OFFICE (JFO) ACTIVATION AND OPERATIONS

Version 7.1
Public availability to be determined under 5 U.S.C. 552Y

Table of Contents

Appendix 1: List of Acronyms **1**

Appendix 2: References **9**

Annex A: Roles and Responsibilities **10**

1.0 Regional Responsibilities 10

Annex B: Administrative Reports **11**

Tab 1 to Annex B: Financial Report Template 12

Tab 2 to Annex B: Closeout Report 13

Tab 3 to Annex B: After-Action and Lessons Learned (Hotwash) Report (LLR) 14

Tab 4 to Annex B: Secretary's Remedial Action Management Program (SEC RAMP) AAR Format 19

Annex C: Operations **20**

1.0 Principles for Building Interagency Coordination 20

2.0 The JFO Coordination and Support Cycle 23

Tab 1 to Annex C: Decisionmaking Process 40

Tab 2 to Annex C: CP Cover Sheet 43

Tab 3 to Annex C: Coordination Objectives 44

Tab 4 to Annex C: Assignment List 45

Tab 5 to Annex C: Assignment List Attachment 46

Tab 6 to Annex C: ICS-209-JFO, Coordination Status Summary 47

Annex D: Logistical Requirements **56**

1.0 Joint Field Office Logistics Requirements (conceptual) 56

2.0 Scenario One: Type I (Major) Disaster 59

3.0 Scenario Two: Type II Heightened Threat of Terrorism w/out WMD 60

4.0 Scenario Three: Type I Heightened Threat of Terrorism w/ WMD 61

5.0 Scenario Four: Type I Federal-to-Federal Support (Spill of National Significance) 62

6.0 Scenario Five: Type III Federal-to-Federal Support (Chemical Release Accident) 63

7.0 JFO Size Requirements Estimation Worksheet 64

Tab 1 to Annex D: Pre-deployment Conference Call Checklist 65

Tab 2 to Annex D: PFO Go Kit Footprint 66

Tab 3 to Annex D: DHS/HSOC Go Kit Footprint 67

Annex E: Communications and Information Sharing **68**

1.0 Purpose and Scope 68

2.0 Intra-JFO Communications 68

3.0 External Communications 71

4.0 Threat Monitoring and Initial Incident Assessment 72
5.0 Daily Production 72
6.0 Secure Video Teleconferences (SVTCs) 73
7.0 Situation Unit Watch Rotations 74
8.0 Logs 74
Tab 1 to Annex E: JFO "Battle Rhythm" Timeline 75
Tab 2 to Annex E: Initial Situation Report (SITREP) 76
Tab 3 to Annex E: Situation Update Reports 77
Tab 4 to Annex E: Urgent Situation (Spot) Reports 79
Tab 5 to Annex E: Threat Situation Report 80
Tab 6 to Annex E: Casualty Reports 83
Tab 7 to Annex E: HSIN-JFOnet Technical Data 85
Tab 8 to Annex E: Template JFO Information-Sharing Plan 86

Annex F: Security Procedures 97
Tab 1 to Annex F: SOP for Information Classification and Handling 98
Tab 2 to Annex F: SOP for Verification of NSCI Clearances 112
Tab 3 to Annex F: SOP for Emergency Disclosure of NSCI 113
Tab 4 to Annex F: SOP for SCI/SCIF Operation 115
Tab 5 to Annex F: Template Physical and Information Security Plan 135
Tab 6 to Annex F: SOP for SBU Information Handling 136

Annex G: Principal Federal Official 140
1.0 Alert and Designation 140
2.0 Roles and Responsibilities 140
3.0 Concept of Operations 141
4.0 Logistical Requirements 151
5.0 Administration and Logistics 152
Tab 1 to Annex G: Reports/Scheduled Events 155
Tab 2 to Annex G: Mission Points of Contact 155
Tab 3 to Annex G: Weather 157
Tab 4 to Annex G: Request for Information 157
Tab 5 to Annex G: Communications Tracking Log 159
Tab 6 to Annex G: Attendance Tracking Log 160
Tab 7 to Annex G: Requests for Information Tracking Log 161
Tab 8 to Annex G: Financial Information 162
Tab 9 to Annex G: Domestic Emergency Support Team (DEST) 163

Annex H: Joint Field Office Organization 164
Tab 1 to Annex H: Sample JFO Organization for Natural Disasters 164

Tab 2 to Annex H: Sample JFO Organization for Terrorism Incidents 165
Tab 3 to Annex H: Sample JFO Organization for Federal-to-Federal Support 166
Tab 4 to Annex H: Sample JFO Organization for National Special Security Events 167

Annex I: Joint Information Center 168

Annex J: JFO Exercise Evaluation Guidelines 169

Appendix 1: List of Acronyms

AAR	After-Action Report
AC/IC	Area Command/Incident Command
ADP	Automatic Data Processing
Air Ops	Air Operations Branch Director
ASIA	Assistant Secretary for Information Analysis
BPA	Blanket Purchase Agreement
CBP	Customs and Border Protection
CBRNE	Chemical/Biological/Radiological/Nuclear/Explosive
CFO	Chief Financial Officer
CIA	Central Intelligence Agency
CI/KR	Critical Infrastructure/Key Resources
CIO	Chief Information Officer
COA	Course of Action
CONOPS	Concept of Operations
COOP	Continuity of Operations Plan
CSA	Cognizant Security Authority
CUL	Cost Unit Leader
CVS	Clearance Verification System
DAN	Document Accountability Number
DCE	Defense Coordinating Element
DCID	Director of Central Intelligence Directive
DCN	Document Control Number

DCO	Defense Coordinating Officer
DCS	Defense Courier Service
DEST	Domestic Emergency Support Team
DFO	Disaster Field Office
DHS	Department of Homeland Security
DISC	Disaster Information Systems Clearinghouse
DOB	Date of Birth
DOD	Department of Defense
DOJ	Department of Justice
DOM	Disaster Operations Manual
DRC	Disaster Recovery Center
DREC	Deputy Regional Emergency Coordinator
DRF	Disaster Relief Fund
DRM	Disaster Recovery Manager
DSCA	Defense Support of Civilian Authorities
DT	Development Team
DTRIM PCC	Domestic Threat Response and Incident Management Policy Coordination Council
DUL	Documentation Unit Leader
EAP	Emergency Action Plan
EC	Emergency Coordinator
EOC	Emergency Operations Center
EMI	Emergency Management Institute (FEMA)
EPA	Environmental Protection Agency
EPL	Evaluated Products List

ERT	Emergency Response Team
ERT-A	Emergency Response Team–Advance Element
ERT-N	National Emergency Response Team
ESF	Emergency Support Function
FAA	Federal Aviation Administration
FAMS	Federal Air Marshals Service
FAR	Federal Acquisition Regulations
FBI	Federal Bureau of Investigation
FCO	Federal Coordinating Officer
FEMA	Federal Emergency Management Agency
FOC	Full Operating Capability
FPS	Federal Protective Service
FRC	Federal Resource Coordinator
FSC	Finance/Admin Section Chief
GAR	Governor's Authorized Representative
GSA	General Services Administration
GSAR	General Services Administration Acquisition Regulations
HHS	Department of Health and Human Services
HSC	Homeland Security Council
HSIN	Homeland Security Information Network
HSIR	Homeland Security Intelligence Report
HSOC	Homeland Security Operations Center
HSOMB	Homeland Security Operations Morning Brief
HSPD	Homeland Security Presidential Directive

IC	Incident Command
ICE	Immigration and Customs Enforcement
ICEP	Incident Communications Emergency Plan
ICP	Incident Command Post
ICS	Incident Command System
IDS	Intrusion Detection System
IIMG	Interagency Incident Management Group
IMP	Immediate Identification Plan
IO	Information Officer
IOC	Initial Operating Capability
IR	Infrared
IT	Information Technology
JFO	Joint Field Office
JFO CG	Joint Field Office Coordination Group
JIC	Joint Information Center
JIS	Joint Information System
JOC	Joint Operations Center
JPAS	Joint Personnel Adjudication System
JRIES	Joint Regional Information Exchange System
JTF	Joint Task Force
JTTF	Joint Terrorism Task Force
JRIES	Joint Regional Information Exchange System
LLR	Lessons Learned (Hot Wash) Report
LNO	Liaison Officer

LSC	Logistics Section Chief
MACC	Multiagency Command Center
MERS	Mobile Emergency Response Support
MOA	Memorandum of Agreement
MOB	Mobile Operations Branch
MOU	Memorandum of Understanding
NCR	National Capital Region
NCTC	National Counterterrorism Center
NGA	National Geospatial Intelligence Agency
NGO	Nongovernmental Organization
NICC	National Infrastructure Coordinating Center
NICCL	National Incident Communications Conference Line
NIMS	National Incident Management System
NISPOM	National Industrial Security Program Operating Manual
NRCC	National Response Coordination Center
NRP	National Response Plan
NSA	National Security Agency
NSI	Classified National Security Information
NSSE	National Special Security Event
OCONUS	Outside the Continental United States
OE	Organizational Element
OPA	Office of Public Affairs
OSC	Operations Section Chief
OSLGCP	Office of State and Local Government Coordination and Preparedness

PA	Public Affairs
PAO	Public Affairs Office/Officer
PDA	Personal Digital Assistant
PDA	Preliminary Damage Assessment
PDD	Presidential Decision Directive
PDS	Practice Dangerous to Security
PED	Portable Electronic Device
PFO	Principal Federal Official
POB	Place of Birth
PSC	Planning Section Chief
PSD	Protective Security Division
RA	Regional Administrator
REC	Regional Emergency Coordinator
RF	Radio Frequency
RFA	Request for Assistance
RFA	Request for Federal Assistance
RFI	Request for Information
RON	Rest Overnight
RRCC	Regional Response Coordination Center
RRR	Readiness, Response and Recovery
RUL	Resource Unit Leader
S&T	Science and Technology
SAAR	Secretary's After Action Report
SAC	Special Agent in Charge (FBI)

SAIC	Special Agent in Charge (USSS)
SBU	Sensitive but Unclassified
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SCO	State Coordinating Officer
SEC RAMP	Secretary's Remedial Action Management Program
SERT	Secretary's Emergency Response Team (HHS)
SFLEO	Senior Federal Law Enforcement Official
SFO	Senior Federal Official
SIOC	Strategic Information and Operations Center (FBI)
SITREP	Situation Report
SMB	Secretary's Morning Brief
SME	Subject Matter Expert
SO	Security Officer
SOIC	Senior Official of the Intelligence Community
SOP	Standard Operating Procedure
SPOTREP	Spot Report
SPSCIF	Semi-Permanent Sensitive Compartmented Information Facility
SSN	Social Security Number
SSO	Special Security Officer
STE	Secure Telephone Equipment
STU	Secure Telephone Unit
SUL	Situation Unit Leader
SVTC	Secure Video Teleconference

SWO	Senior Watch Officer
TAIS	Telecommunications and Automated Information Systems
TIMACS	Telecommunications Information Management and Control System
TLC	Territory Logistics Center
TSA	Transportation Security Administration
TSC	Terrorist Screening Center
TSCA	Top Secret Control Account
TSCM	Technical Surveillance Countermeasures
TSCO	Top Secret Control Officer
TS/SCI	Top Secret/Sensitive Compartmented Information
TSWA	Temporary Secure Working Area
UC	Unified Command
USACE	United States Army Corps of Engineers
USCG	United States Coast Guard
USSOCOM	US Special Operations Command
USSS	United States Secret Service
WMD	Weapons of Mass Destruction

Appendix 2: References

- DEST Memorandum of Understanding (MOU) between DHS and FBI
- Homeland Security Act of 2002
- Homeland Security Operations Center (HSOC) SOP
- Homeland Security Presidential Directive-5
- Homeland Security Presidential Directive-7
- Homeland Security Presidential Directive-12
- Interagency Incident Management Group (IIMG) SOP
- National Incident Management System (NIMS)
- National Response Plan (NRP)
- Presidential Decision Directive-39
- Presidential Decision Directive-62
- Robert T. Stafford Disaster Relief and Emergency Assistance Act

Annex A: Roles and Responsibilities

1.0 Regional Responsibilities

1.1 JFO Developmental Organizations.

To facilitate the development of future JFOs and other DHS facilities for each high-threat or regional area, a JFO Development Team (DT) will be established. This team will be co-chaired by the appropriate DHS/FEMA regional office, DHS/USSS field office, and/or FBI field office. Membership of the team will include all DHS field elements within the defined urban threat area or regional area. DHS/FEMA will coordinate general oversight and guidance throughout the process, ensuring that the years of experience and existing assets utilized in the development of DFOs are carefully integrated into the JFO developmental process. The Under Secretary of Preparedness will assign organizational responsibility to the appropriate DHS/FEMA elements to ensure oversight of the process.

1.2 Regional JFO Development Team Taskings

1.2.1 Develop a JFO Strategy consistent with:

- JFO SOP
- NSSE requirements
- Threat environment
- Demographics
- Existing political structure
- Level of local and State readiness and operational systems
- Existing regional Federal structure

1.2.2 Develop JFO staffing plans, consistent with the JFO SOP, supporting all organizational elements of a fully functional JFO for the specific regional area. These plans should identify the organizations or representatives from the appropriate DHS elements needed to maintain the JFO readiness posture once established for each region or urban threat area.

1.2.3 Develop a JFO IMP. In addition to pre-identification of facilities, each DT should develop a JFO Immediate Identification Plan (IMP) to support any activation resulting from a threat, actual incident, or NSSE. This plan should be activated/implemented in the event of a WMD incident and in the absence of an available pre-selected site. It would provide a critical action plan that provides Federal, State, local, and private-sector contacts with those organizations that have previously agreed to support the accelerated development of a JFO. The general sizing requirements based on the incident type, asset, and communication requirements should also be included.

Annex B: Administrative Reports

Tab 1 to Annex B: Financial Report Template

[RESERVED]

Tab 2 to Annex B: Closeout Report

[RESERVED]

Tab 3 to Annex B: After-Action and Lessons Learned (Hotwash) Report (LLR)

1.0 General

The After-Action Report is a narrative summary of the operations, contingency response, or exercise. An AAR may contain specific associated lesson(s) learned and primarily:

- Summarizes JFO operations or exercises,
- Assesses how well the NRP's objectives were accomplished, and
- Documents major lessons learned for followup action, including action by the Secretary of Homeland Security through the SEC RAMP.

The Planning Section Chief is responsible for initiating the AAR/LLR process prior to demobilization of the Planning Section. The PFO/FRC/FCO, as appropriate, is responsible for overseeing the AAR/LLR process in a manner to comply with the deadline.

The Lessons Learned (Smart Practice) Report is a standalone record that documents specific issues, problem areas, best practices, and work-arounds pertaining to operations, contingency response, or exercises. Each lesson learned should be prepared so that it does not rely on another part of the document (AAR/LLR) for clarification. The AAR for the JFO does not replace separate agency after-action processes. The JFO AAR may be integrated into agency-specific after-action systems. AARs/LLRs pertaining to the JFO established for a NSSE will address only the JFO and NRP aspects of the operation.

2.0 Objective

The objective of the JFO AAR/LLR process is to provide an assessment of JFO effectiveness during the Incident of National Significance response or exercise. It includes a brief mission description and significant events, discussion of interoperability with other organizations, and recommendations. It may identify areas for improvement in homeland security doctrine (i.e., policy, procedures, plans, and tactics) and training. Individual lessons learned may be attached to the AAR, providing a more comprehensive picture of the response or exercise. Individual LLRs are used to describe a better way of accomplishing a task or overcoming a problem, describe a successful action that should be noted for future contingencies, describe a problem encountered and the action the participants took to bypass or alleviate that problem, or document an issue that was encountered for which no solution was found.

3.0 Requirements for Submission

The JFO AAR/LLR should be completed and forwarded to arrive at the DHS/Office of Operations Incident Management Division (IMD) within 60 days of JFO stand-down and should be in the format outlined below.

4.0 AAR Format

4.1 Identifying Information

This section provides standard information to index and identify the report and document submission of the AAR.

4.1.1 Incident of National Significance Name

This is the name given to the operation, response, or exercise, such as Desert Storm, Positive Response Y2K, Exxon Valdez, Hurricane Andrew, etc.

4.1.2 Type of Incident of National Significance

This is the specific NRP Incident of National Significance criterion which caused the activation of the NRP and JFO.

4.1.3 Point of Contact

Name of person and home organization of the person submitting the AAR.

4.1.4 Expenditures

Actual expenses made through the JFO against all applicable NRP-activated funds.

4.2 Executive Summary

This section should contain a concise summary of JFO and NRP-related strategic and operational highlights while addressing areas for improvement in effectiveness, efficiency, coordination, and interoperability.

4.3 JFO Coordination and Support Operations

This section should be used to discuss specific JFO and NRP operational issues in the following areas:

4.3.1 Command Center Interoperability, Communication, and Information

(essentially C3I)

4.3.2 Intelligence Issues

(threat assessment, vulnerability evaluation, consequence assessment, integrated risk-based decisionmaking, quality and capability of dissemination of information);

4.3.3 Coordination Planning Issues and Activities

(coordination cycle implementation, support operations, coordination activities);

4.3.4 Security Issues

(information classification and handling, physical security, badging and access control, emergency disclosure, operation of SCIFs);

4.3.5 National Response Plan Issues

(deriving from the NRP itself); and

4.3.6 Statistical Data

such as support assets provided, JFO-related aircraft sorties/hours, and law enforcement activities.

4.4 JFO Support

This section should address specific JFO support issues such as planning documents and SOPs, personnel requirements, logistics/supplies requirements, financial issues, legal issues, and external affairs (including media affairs) items.

4.5 NRP and JFO Objectives and Major Lessons Learned

This section should address how well the NRP and JFO objectives were met during the operation, response, or exercise.

4.6 Limitations and Accidents

This section should detail any factor that limited full accomplishment of NRP and JFO objectives and should detail any JFO-related accidents, injuries, or deaths.

4.7 Participants

This section should identify the coordinating entities involved in JFO operations.

5.0 LLR Format

5.1 Incident of National Significance Name

This is the name given to the operation, response, or exercise, such as Desert Storm, Positive Response Y2K, Exxon Valdez, Hurricane Andrew, etc.

5.2 LLR Identifying Information

The identifying information associated with each lesson learned is very important for retrieving lessons learned by a number of categories. See the QUICK HITTER Lessons Learned Capture Worksheet at the end of this tab.

5.2.1 Lesson Learned Title

This is not the same as the event name. It should be something that can be easily recognizable as the main theme of the lesson learned.

5.2.2 Recommended Action

This should be a short description of what the author has concluded should be done as follow-on action. If the lesson learned contains a recommendation for follow-on action, then the author should so indicate here. If action was recommended and has since been taken, then "no further action" should be noted. If the lesson learned requires no action, then it should be characterized as "for information only."

5.2.3 Observation Capture Date(s)

This should record the date(s) on which the lesson learned was observed in the field or at the JFO.

5.2.4 Type of Incident of National Significance

Choose the contingency that was supported during the event.

5.2.5 NRP or ICS Category

Choose the NIMS ICS position or function from the LLR Worksheet on page 22 that would most likely deal with the theme of the lesson learned. The NRP and NIMS are good references for deciding the best NRP category or ICS position to choose.

5.2.6 Plan Component

This category helps define the lesson learned in the context of what component of a plan (if any) was being exercised or executed when the lesson learned observation was made.

5.2.7 Recommended Action Area

Choose what area is the best place to implement the recommendation of the lesson learned. This is especially important because it places the lesson learned in the context of how best to improve performance, prevention, plans, and policy, which is one of the primary reasons for collecting and disseminating lessons learned.

5.3 Observation

Should contain a brief factual statement of the observed success or problem. Statement can be (1) positive about something done exceptionally well or about procedures used that should be shared, or (2) negative about something that happened that should not have occurred or something that did not occur but should have.

5.4 Discussion

Should amplify the success or problem described in the observation. Should answer the questions "Who, What, When, Where, Why, and How."

5.5 Lesson Learned (Smart Practice)

Should contain information on the positive action taken to generate success or the action that should be taken to avoid or alleviate or work around a problem.

5.6 Recommendation

Should contain a statement of how to repeat the success or permanently correct the problem and who should make the correction. The recommendation could result in a requirement for new or modified publication, procuring new equipment, changing force structure, revising command relationships, or improving training.

Joint Field Office QUICK HITTER Lessons Learned Capture Worksheet					
Topic			**Date Observed / Lesson Captured**		
Type of Incident of National Significance:					
Recommended Action:					
☐ Follow-on Action needed	☐ Information Only				
☐ Follow-on Action completed	☐ Other Recommended Action				
☐ Smart Practice					
NRP or NIMS ICS Category:					
☐ JFO Coordination Group	☐ JFO Logistics Section		☐ NRP Function Annexes		
☐ PFO / FCO / FRC / FC	☐ JFO Finance / Admin Section		☐ NRP Incident Annexes		
☐ PFO Support Staff	☐ JFO Joint Information Center		☐ HSOC Interface		
☐ JFO Coordination Staff	☐ JFO Security		☐ Command Posts		
☐ JFO Operations Section	☐ NRP Base Plan		☐ Other Category		
☐ JFO Planning Section	☐ NRP Support Annexes				
Relevant Plan or SOP Component					
Plan	Component				

Observation. A brief factual statement of the observed success or problem; can be (1) positive about something done exceptionally well or procedures used that should be shared, or (2) negative about something that happened that should not have occurred or something that did not occur but should have.

Discussion. Amplify the success or problem described in the observation; answer the questions "Who, What, When, Where, Why, and How."

Lesson Learned (Smart Practice). Information about the positive action taken to generate success or the action that should be taken to avoid, alleviate, or work around a problem.

Recommendation. A statement of how to repeat the success or permanently correct the problem, who should make the correction, and the area in which it should be made. The recommendation could result in a requirement for new or modified publication, procuring new equipment, changing personnel structure, revising command relationships, or improving training.

Tab 4 to Annex B: Secretary's Remedial Action Management Program (SEC RAMP) AAR Format

[RESERVED]

Annex C: Operations

1.0 Principles for Building Interagency Coordination

Interagency coordination and cooperation is critical to effective and efficient operations to preempt or mitigate natural or man-made disasters. It is imperative that representatives of agencies with diverse capabilities synchronize their efforts through the application of basic teaming principles. These principles, shown below, support a systematic methodology toward building a homogeneous effort at all levels of government.

1.1 Define the Problem in Clear and Unambiguous Terms Agreed to by All

Differences in individual assumptions and organizational perspectives can often limit clear understanding of the problem. Representatives from each major group of agencies, departments, and organizations—to include the on-scene Incident Command agencies—should be involved in all levels of coordination planning from the outset. These representatives are especially important in order to achieve unity of effort during this problem definition phase; early development of options for interagency consideration is very important. Not all agencies and individuals clearly distinguish in the same way between wide-area operational coordination and incident command-and-control or oversight. Defining the problem that the JFO solves should involve extensive focus on the difference between wide-area operational coordination and command-and-control over the incident itself.

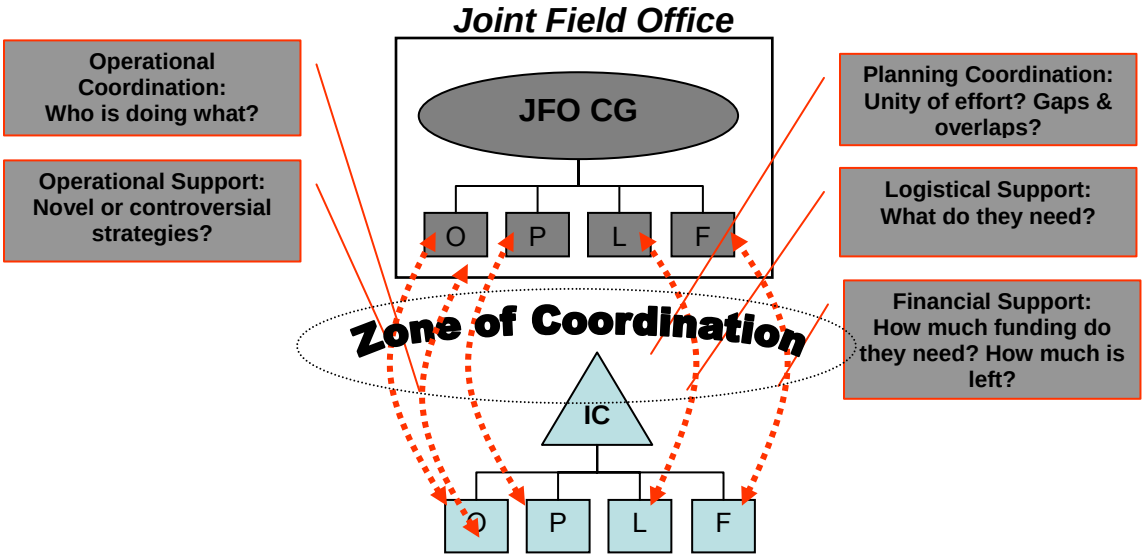
1.2 Define the Objectives

Within the context of interagency operations, decisionmakers in the JFO Coordination Group should seek clearly defined and attainable objectives, a concrete end state, and exit criteria. Successful interagency coordination is essential to achieve these goals and the development of accurate and timely assessments. Such definition allows application of resources of the most appropriate agency(s). Not all agencies will necessarily understand or agree to the need to clearly define the objective with urgency or specificity. Complications can arise because each agency has its own perspective, capabilities, and culture. This diversity is the strength and not the weakness of the interagency coordination process. While there may be disagreement about solutions, the differences provide a broad range of options that can be applied.

1.3 Operations Drive at Tactical Level; Logistics, Situation, and Planning Drive at Strategic Level

At the field or tactical level, an Incident Command surges in as operations are already occurring; everything in the Incident Command serves to support operations. At the strategic level, coordination of operations typically follows in-depth development of the situation in the "wide area," answering of requests for logistics support, and digestion/consolidation of

incident and coordinating agency plans of action. In the "zone of coordination" between the Incident Commander(s), local EOCs, and the JFO (see figure below), logistics, situation, and planning should drive coordination.



1.4 Establish a Common Frame of Reference

The interagency environment can become complicated by differences in key terminology. The meaning of the terms "safe zone" or "operations" to one agency may have somewhat different connotations to another. This misunderstanding may cause operational impacts. The semantic differences commonly experienced within a given Federal department may grow in the interagency arena, particularly in broad interdisciplinary incident responses. JFO staff must anticipate possible semantic mismatches and take measures to clarify and establish common terms with clear and specific usage.

1.5 Develop Courses of Action or Options

These should address the problem and achieve the objectives. JFO staff should focus their efforts on their agency's enabling capabilities that contribute to coordination objective attainment and are part of the interagency plan of action. Resource-sensitive problems require good options to lead to good solutions. Providing too few or clearly impractical options or recommending the "middle of the road" approach merely for the sake of achieving consensus is of little service to decisionmakers. The synergism of open debate within the interagency community produces the best options.

1.6 Capitalize on Experience

Review after-action reports and lessons learned to assess proposed courses of action and to reduce the requirement to learn on the job. Though their lessons learned systems differ in scope and nature, almost all agencies have their own systems in place to capitalize on operational experience. These should be sought and used in all cases prior to the beginning of JFO operations. Lessons learned must be captured throughout the duration of the JFO's operation and documented in the After-Action and Lessons Learned Report described in Tab

3 to Annex B of this SOP.

1.7 Establish Responsibility

When all participants in the interagency process understand what needs to be done, agree upon the means to accomplish it, and identify who will do what through coordination, a common sense of ownership and commitment toward resolution help achieve unity of effort. The resources required for a mission must be painstakingly identified, with specific and agreed-upon responsibility assigned to the agency(s) that will provide those resources. To receive proper reimbursement for materiel support, agencies must establish careful accounting procedures.

1.8 Plan for the Transition of Key Responsibilities, Capabilities, and Functions

Immediately upon initiating interagency coordination, it is imperative to plan for the transition of responsibility for specific actions or tasks from emergency to more routine entities. This planning usually occurs simultaneously at the national level. When interagency transition planning (including assignment of specific responsibilities and timelines for accomplishment) does not occur, JFO involvement may be needlessly protracted. As coordination plans are developed at the JFO Coordination Group level, effective transition planning should also be a primary consideration. The JFO Coordination Group should anticipate the need to "ratchet down" coordination and/or direct incident support to lessen the impact of transitioning to other "routine ops" organizations.

1.9 Direct All Means Toward Unity of Effort

Achieving unity of effort can be made more complex by the number of participants, distinctive agency cultures, undefined relationships among the agencies, and differing objectives. The principle of unity of effort pertains directly to interagency coordination. Unity will lead to success for the mission, not a zero-sum equation among the agencies. Achieving this principle begins by identifying agencies that have the requisite capabilities to reach the common objective or a need to adapt their wide-area operations in light of the incident response and by bringing their core competencies to the interagency forum. Because the principles of Unified Command apply to the JFO Coordination Group, the objectives are a reflection of the agencies' collective approach rather than "tasking" from a senior commander. Concerns of national authorities and the IIMG may well be conveyed to the JFO Coordination Group and may ultimately influence the JFO Coordination Plan objectives.

1.10 Media Impact on Interagency Coordination

The formulation and execution of any policy must consider the public's traditional values if the policy is to be successful. The media can be a powerful force in shaping public attitudes and policy development. The media often has a dramatic influence on the interagency process—whether at the strategic decisionmaking level of the IIMG or in the field as agencies and NGOs vie for public attention. Coordination plans that include interaction with these agencies should anticipate the importance that public affairs and media relations have on the operation and in the interagency process. As early as possible in the planning process,

all participating agencies and organizations need to establish and agree on procedures for media access, issuing and verifying credentials, and briefing, escorting, and transporting media members and their equipment. Common communication points and public affairs themes should be developed as quickly as possible so that organizations are not perceived by the media as working at cross purposes with one another. Responsibility for interaction with the media should be established clearly so that, to the extent possible, the media hears from a single voice. ESF #15 has primary responsibility for developing and executing the public affairs strategy, in close coordination with DHS Public Affairs. ESF #15 is also responsible for establishing the JIC.

2.0 The JFO Coordination and Support Cycle

2.1 Initial Coordination, Support, and Assessment

Initial Coordination and Assessment occurs in all incidents. Short-term coordination efforts, which are small in scope and/or duration (e.g., a few agencies supplying only a few resources to the Incident Command on-scene and completing adaptive changes to their routine operations surrounding the incident in one coordination period) can often be coordinated without developing a full Coordination Plan using only Initial Situation Reports (see Tab 2 to Annex E of this SOP). The extent of the JFO role in resource and logistics support may vary depending on the needs of the ICP and funding mechanisms being used for the incident.

2.1.1 Coordination Briefing (Situation Report and Agency/Incident Coordination Plans)

During the transfer of coordination responsibilities, a coordination briefing based on the existing situation reports and Coordination Plans obtained through appropriate Federal, State, and local channels from Incident Commanders, Area Commanders, EOCs, coordinating agencies, and the ERT-A, if deployed, will provide the incoming JFO Coordination Group (or initial coordinating agency) with basic information regarding the incident situation, resource support requested, and relevant "wide-area" operations that have been adapted because of the incident. Most importantly, the coordination briefing and situation report function as the Coordination Plan for initial coordination and support and remain in force and continue to develop until the coordination effort ends or the JFO Planning Section generates the first Coordination Plan. The coordination briefing and situation report is also suitable for briefing individuals newly assigned to the JFO Coordination Staff as well as needed assessment briefings for the staff.

The required situation report documents coordinated "wide-area" coordination objectives, incident support objectives, situational awareness, resource requests and deployment, and significant actions taken. This form is essential for future planning and the effective management of initial response activities.

When: New JFO Coordination Group, PFO/FCO/FRC; staff briefing as required
Facilitator: Current Federal incident coordinator(s) (e.g., DHS/FEMA, FBI, DHS/USSS, other)
Attendees: JFO Coordination Group; JFO Coordination Staff (equivalent to the Unified Command Staff) and JFO Section Chiefs (equivalent to the Unified Command General Staff).

General Tasks

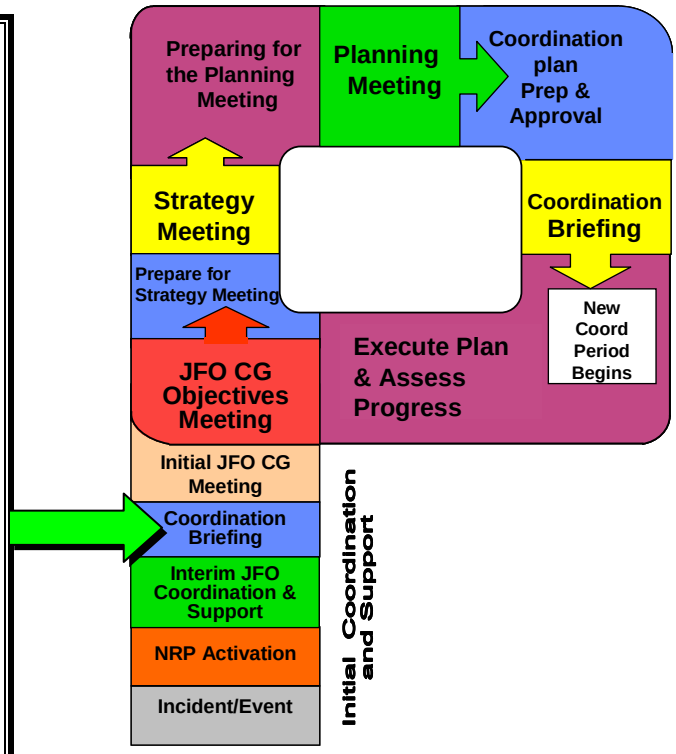
JFO CG
- ❑ Obtain coordination brief.
- ❑ Assess organizational and support requirements and objectives.
- ❑ Consider future coordination requirements and objectives.

JFO OSC
- ❑ Obtain briefing from lead coordinator State, Federal, tribal, and local EOCs.
- ❑ Conduct operation support in current coordination period as requests arise.

JFO PSC
- ❑ Brief Situation, Coordination Plans in effect.
- ❑ Consider available Contingency Plans.
- ❑ Document, evaluate, and develop strategies.

JFO LSC
- ❑ Brief Resource Requests.
- ❑ Consider available resources.

JFO FSC
- ❑ Brief Funding Expenditures and Ceiling.



- Agenda. Using the Situation Briefing and/or Coordination Plan template as an outline, include:
  - Consolidated situation from all agencies/Incident Commanders (note territory, exposures, safety concerns, etc.; use map/charts).
  - Synopsis of current agency and Incident Commander objectives.
  - National strategy and areas of concern from the IIMG.
  - Synopsis of all agencies' and Incident Commanders' strategies in effect, including on-scene response strategy (from collected ICS Form 201s or Coordination Plans).

- Readily apparent gaps, seams, and overlaps in consolidated Objectives and Strategies.
- Tactical/Response Resources requested from the JFO, en route and/or ordered.
- Summary all known Agency and Incident Commander Resource assignments (recognizing this will be incomplete initially).
- Current JFO coordination and support organization.
- Facilities established (particularly COOP sites or candidates for the JFO).

2.1.2 Initial JFO Coordination Group Meeting

This meeting provides the JFO Coordination Group with an opportunity to discuss and concur on important issues prior to coordination and to support incident action planning. The meeting should be brief and important points documented. Prior to the meeting, JFO Coordination Group members should have an opportunity to review and prepare to address the agenda items. Planning Meeting participants will use the results of this meeting to guide coordination and support efforts prior to the first Strategy Meeting.

When: Typically this meeting occurs immediately after the first Coordination Briefing to the JFO Coordination Group.
Facilitator: PFO/FCO/FRC or designee
Attendees: Only JFO Coordination Group members

General Tasks

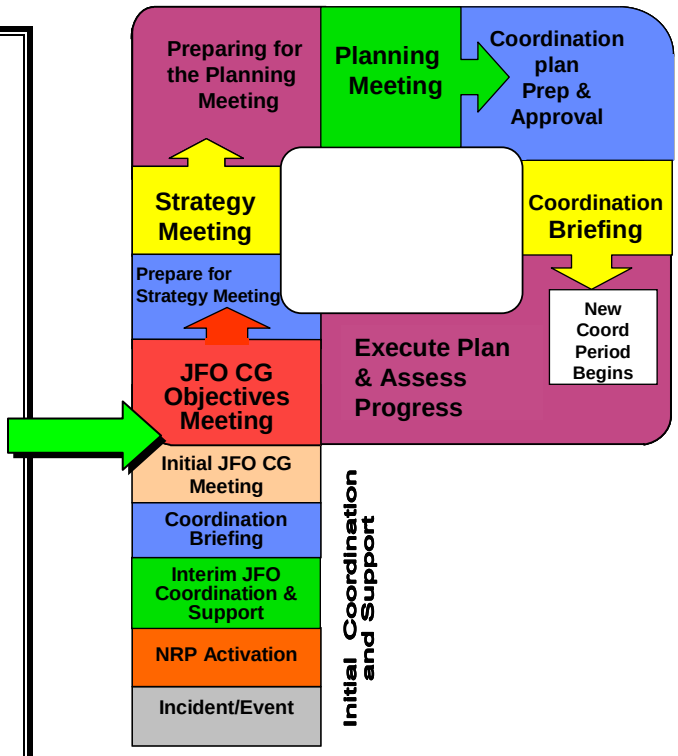
JFO CG
- ❑ Identify additional JFO CG members.
- ❑ Negotiate/facilitate JFO participation.
- ❑ Clarify JFO CG roles and responsibilities.
- ❑ Negotiate and agree on coordination organization, facilities, and support.
- ❑ Synchronize Coordination Period length/start time.

JFO OSC (if requested)
- ❑ Brief JFO CG members on current coordination and operational support.

JFO PSC (if requested)
- ❑ Brief JFO CG members on current situation, planning coordination, and technical support.

JFO LSC (if requested)
- ❑ Brief JFO CG members on current coordination and logistical support.

JFO FSC (if requested)
- ❑ Brief JFO CG members on current coordination and logistical support.



- Agenda.
  - Identify JFO Coordination Group members and potential members, based on NRP criteria.
  - Identify JFO Coordination Group agency and Incident Commander support and coordination objectives.
  - Present jurisdictional limitations, concerns, and restrictions.
  - Develop a collective set of support and coordination objectives.
  - Establish and agree on JFO Coordination Group consolidated support and coordination priorities.
  - Verify that Incident Commanders, Area Commands, EOCs, and coordinating agencies have been informed they can "outsource" technical assistance requests to the JFO rather than importing redundant tech specialists to each ICP/operations center (i.e., avoid unnecessary competition for scientific and other technical resources).
  - Agree on basic JFO section organization structure.
  - Agree on JFO Coordination Staff and JFO section personnel designations and operations, planning, logistical, and financial agreements and procedures.
  - Agree on unified logistics approach to resource ordering (support) procedures to follow.
  - Agree on cost sharing/mission assignment or authorization procedures.
  - Agree on informational matters.
  - Designate a JFO External Affairs Officer.

- Identifying Additional JFO Coordination Group Members. During the initial JFO Coordination Group meeting, a key task is identifying all agencies, departments, and organizations that are or should be involved in developing and executing the wide-area strategy and/or in supporting the on-scene Incident Commander. This analysis needs to include identification of the participating NGOs and private-sector organizations. In many cases, initial planning and coordination have occurred in Washington, DC, so the PFO/FCO /FRC should ensure that the JFO staff are made aware of all the agencies to be involved in the mission.

- Clarifying Interagency Relationships. Similarly, during the initial JFO Coordination Group meeting, a second key task is clarifying an authoritative interagency relationship based on the NRP Annexes, considering the coordinating agency identified in the NRP or by national authorities, and determining the cooperating agencies within the JFO Coordination Group. Establishing such an interagency hierarchy may be more or less complex based on interagency player familiarity with the NRP. Nonetheless, the JFO Coordination Group should attempt to insert discipline, responsibility, and rigor into the process in order to function effectively. In many cases, the JFO Coordination Group will discover that information and concurrence of perception will smooth the process, both of which

are established by ensuring constant communication between and among all concerned parties. Regardless of the Coordination Group's efforts to foster coordination and cooperation, critical issues may arise that must be forwarded for resolution to the IIMG.

- Synchronizing the Coordination Period. Typically the on-scene Incident Command will have established coordination periods before (or at least concurrent with) the establishment of a JFO. In this case, because requests for resources in the **next** coordination period will flow up to the JFO following the on-scene Incident Command's tactics meeting, the JFO should carefully consider delaying the start of the JFO Coordination Period such that these resource requests are briefed during the JFO Coordination Group Objectives Meeting. This will put the JFO slightly "out of phase" with the on-scene Incident Command but may better support on-scene logistical needs.

  Similarly, the information cycle outlined in this document should not, in itself, drive the start and length of the JFO Coordination Period. Instead, the information requirements should be viewed as output products which can be tasked for production in the Coordination Plan (via ICS Form 204 or other tasking) to the appropriate JFO organizational element. Where national-level demands for completed wide-area strategy are required, however, the JFO Coordination Group must consider this in synchronizing the JFO Coordination Period.

  Finally, coordination and support missions tend to be more strategic than tactical, with "operationalizing" (putting into operational orders, then tactical execution) and fruition occurring on a much longer timeframe than the on-scene tactical operation. For this reason, the JFO Coordination Group may find itself synchronizing closely to the on-scene Incident Command coordination period early in the incident response, and shifting as the incident progresses to longer (more strategic) Coordination Periods.

2.2 Full Coordination and Support

2.2.1 JFO Coordination Group Objectives Meeting

The JFO Coordination Group will identify/review and prioritize objectives for the **next** coordination period. Support and coordination objectives from the previous coordination period are reviewed and any new objectives are identified.

When: Prior to Strategy Meeting.
Facilitator: PFO/FCO/FRC or designee
Attendees: JFO Coordination Group members; JFO Coordination Staff and sections as appropriate

General Tasks

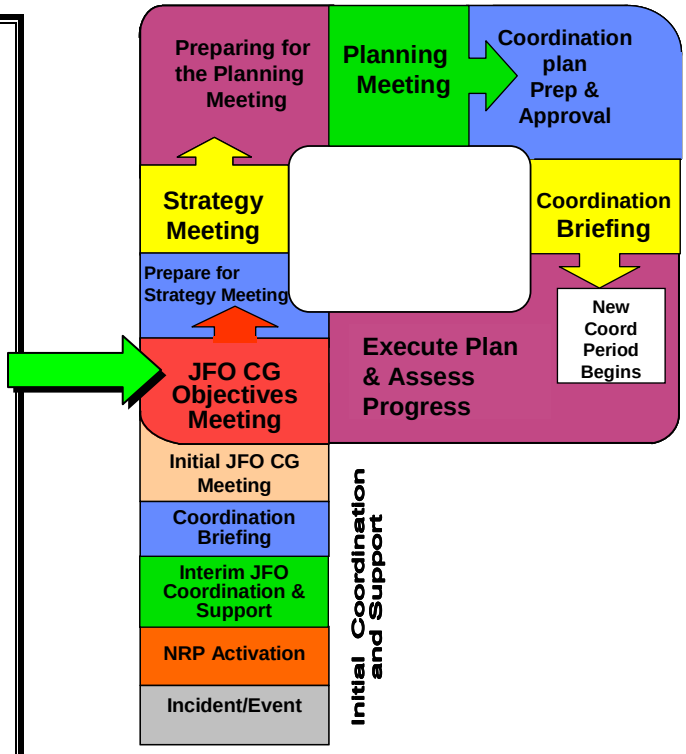
JFO CG
- ❑ Develop coordination and support objectives.
- ❑ Consider all national interest areas.
- ❑ Delegate and provide guidance to Coordination Staff and Section Chiefs.
- ❑ Consider Continuity of Operations and Exit Strategy/Demobilization.

Operations Section Chief (OSC)
- ❑ Summarize operational coordination and support objectives not likely to be completely attained within current Coordination Period.

Planning Section Chief (PSC)
- ❑ Summarize planning coordination and support objectives not likely to be completely attained within current Coordination Period.
- ❑ Identify gaps, seams, and overlaps.
- ❑ Propose draft objectives to JFO CG members.

Logistics Section Chief (LSC)
- ❑ Summarize logistical coordination and support objectives not likely to be completely attained within current Coordination Period.
- ❑ Summarize requests for support.

Finance/Admin (FSC)
- ❑ Summarize financial coordination and support objectives not likely to be completely attained within current Coordination Period.



- Agenda.
  - Review coordination and support objectives from JFO operations, planning, logistics, and finance unlikely to be completely attained in the current Coordination Period and thus carried over to the next.

- Identify issues, concerns, and improvements allowing attainment of coordination and support objectives within targeted timeframe.
- Review, consider, and prioritize requests for support for next Coordination Period.
- Review consolidated list of agency "trigger points" and criteria for engaging or altering operations. Review interagency information flow in view of these critical information requirements.
- Review and identify operational gaps, seams, and overlaps in consolidated national response to the Incident of National Significance.
- Identify objectives for the next Coordination Period (clearly stated and attainable with the resources available, yet flexible enough to allow coordinating agencies, Incident Commanders, and Section Chiefs to choose strategies). Objectives will typically focus on closing gaps, eliminating overlaps, and smoothing transitions at seams in the response.
- Review any open agenda items from initial/previous meetings.

- Agency Perception of the Problem and Priorities. Solicit from each agency, department, or organization a clear definition of the role that each plays in wide-area operations. The understanding of operating principles, legal issues, shortage of capabilities, points of contact, emergency management organization, Presidential/IIMG direction (if applicable), and issues or tasks that cannot be undertaken may well affect mission success. An excellent starting point is to consider what types of information would cause a given agency to change or adapt its wide-area operations/strategy in view of the incident. This information helps build the information-sharing process within the JFO and clearly indicate the agency's view of the problem.

- Obstacles to Unity of Effort. Identify potential obstacles to the collective effort arising from conflicting departmental or agency priorities. Early identification of potential obstacles and concurrence as to solutions by all participants is the first step toward resolution. History demonstrates that obstacles are frequently identified too late in the process and become nearly insurmountable for the on-scene commander. Too often these obstacles are assumed to have been addressed by another agency, department, or organization. Once identified, if the obstacles cannot be resolved at the JFO level, they must immediately be elevated for expeditious resolution.

- Gaps, Seams, and Overlaps. While there is absolutely no authority within the NRP to force or coerce any member agency in the JFO to change or adapt its priorities or objectives, agencies typically adapt willingly when clear gaps in the overall objectives are identified, when seams (i.e., transitions in responsibility) are found problematic, and where overlapping objectives/priorities are apparent. This is the essential purpose of producing unified objectives within the coordination and support framework. Accordingly, the creation of JFO Coordination Group unified coordination and support objectives is more than a cataloging of various agency priorities: it is also a substantive analysis (and correction) of gaps, seams, and

overlaps in objectives and priorities to produce the best and most agile and effective national response possible.

- Continuity of Operations, Transition of Responsibilities, and "Exit Strategy." The safety, security, continuity of operations, and (eventual) transition of responsibilities and demobilization of the JFO should be an immediate concern of the JFO Coordination Group. During massive response operations, such priorities will often appear to be secondary, but excessive delay in tasking the Section Chiefs with specific objectives in these areas may place the continuity of the national response in jeopardy and/or unnecessarily tax national resources with inefficient operations.

- Interagency Information Management. Nongovernmental, private-sector, and regional and international organizations may possess considerable information that may be essential to the success of the coordination and support operation. Relief workers have a comprehensive understanding of the needs of the population. Working closely with local communities, they understand local culture and political organizations. As a consequence, nongovernmental and private-sector organizations are an important source of information regarding the following:
  - Historical perspective and insights into factors contributing to the situation at hand.
  - Local political structure, political aims of various parties, and the role of key leaders.
  - Security situation.

  Handled properly, nongovernmental and private-sector organizations will be active participants in the interagency team seeking to resolve the crisis. Handled improperly, these organizations can be alienated by a perception that, contrary to their organization's mission, they are considered no more than an information source by the Federal Government.

2.2.2 Prepare for the Strategy Meeting

This period of time allows the staff to create and evaluate a series of strategy options (courses of action) for strategic deployment, operations, and support during the **next** coordination period. It is not a meeting. In preparation for the Strategy Meeting, the JFO Planning Section Chief and JFO Operations Section Chief review the unified JFO Coordination Group coordination and support objectives, the first stage of coordination and support operations and/or the current Coordination Plan situation status information as provided by the Situation Unit to assess work progress against the current coordination period's objectives. At the strategic level (where the JFO functions), strategies will be implemented by being translated first into coordinated plans and then into tactical action. The translation into tactical action plans occurs at the IC level, and the JFO Coordination Group monitors strategic implementation. Following up on this two-step agency and/or Incident Commander implementing process is important to monitoring the implementation of JFO coordinated strategy. The JFO Operations Section

Chief/Planning Section Chief will jointly develop primary and alternate strategies to meet coordination and support objectives for selection and development at the Strategy Meeting. To preclude organizational "group think," the JFO Planning Section Chief's primary role will be in developing "devil's advocate" positions on the various strategies, including risk-based evaluations (operational risk management, probability of success, etc.).

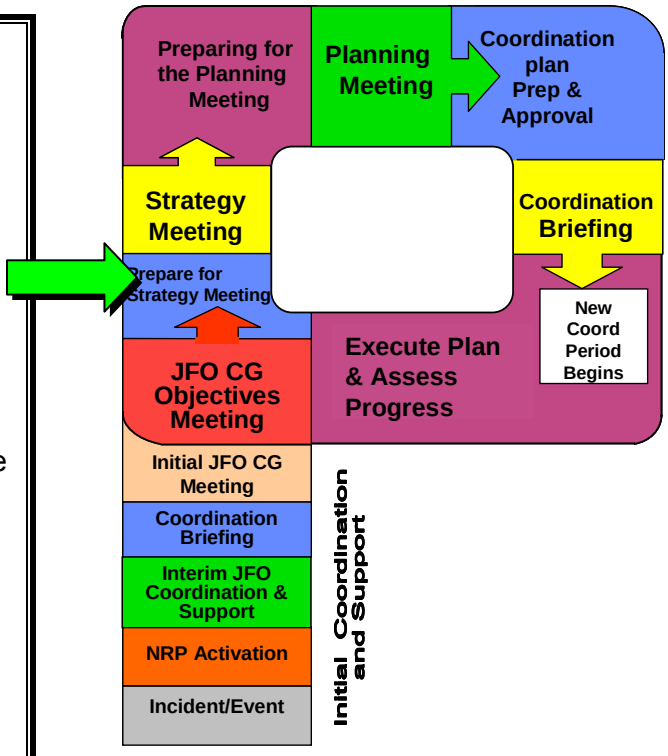
General Tasks

JFO OSC:
- Assemble various courses of action (COAs) from all agency components in Operations
- Evaluate strategic difficulty and timeline to execute for COAs.
- Consider unintended consequences of various agency COAs.
- Select recommended strategy/COA.

JFO PSC:
- Through Situation Unit Leader, assemble status of various agencies in "operationalizing" agreed upon current period strategies.
- Develop "devil's advocate" positions on COAs.
- Consider synchronization to and impact on on-scene resource needs.
- Integrate resource provision strategies with wide-area operational strategies.

Logistics Section Chief (LSC):
- Normally no role.

Finance/Admin
- Normally no role.



2.2.3 Strategy Meeting

This short meeting identifies the coordinated agency strategies; evaluates for additional gaps, seams, and overlaps; and creates the blueprint for "wide-area" strategic deployment and operations during the next coordination period.

When: Prior to Planning Meeting
Facilitator: JFO PSC
Attendees: JFO PSC, JFO OSC, JFO LSC, JFO Resource Unit Leader (RUL), JFO FSC (and others, e.g., EAO)

General Tasks

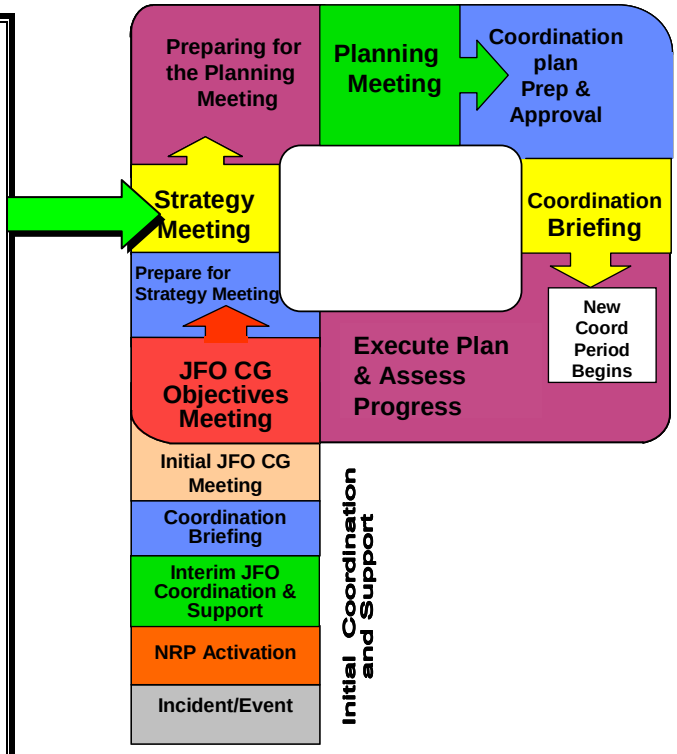
JFO CG:
- ❑ Provide guidance/clarification.

JFO OSC:
- ❑ Be prepared!
- ❑ Brief current strategy status (don't get tactical!).
- ❑ Develop strategies and resource needs (use most effective support tracking tool available).
- ❑ Document JFO resource needs using ICS-215.

JFO PSC:
- ❑ Facilitate meeting.
- ❑ Determine support requirement and logistics tasks.
- ❑ Determine JFO support requirements on ICS-215.
- ❑ Consider alternative and "devil's advocate" strategies.

JFO LSC:
- ❑ Participate /contribute logistics information as necessary.
- ❑ Verify support requirements.

JFO FSC:
- ❑ Evaluate funding implications of each COA/strategy.



- Agenda.
  - Review the support and coordination objectives for the next coordination period and develop strategies (primary and alternative).
  - Prepare support strategy resource needs (i.e., resources to field entities) and document on resource support tracking system for ordering through JFO Logistics.
  - Prepare a draft of ICS Form 215 (used in planning meeting) to identify JFO-internal resources that should be ordered through JFO Logistics.

2.2.4 Prepare for the Planning Meeting

This is not a meeting but a period of time to prepare for the presentation of the Coordination Plan at the Planning Meeting. Each Section Chief is responsible for ensuring that his/her Planning Meeting responsibilities are met. The JFO Planning Section Chief should facilitate this to the greatest extent possible to ensure that the material, information, resources, etc., to be used or discussed in the Planning Meeting are

organized and prepared. There are to be no surprises in the Planning Meeting.

When: After the Strategy Meeting
Facilitator: JFO PSC

General Tasks

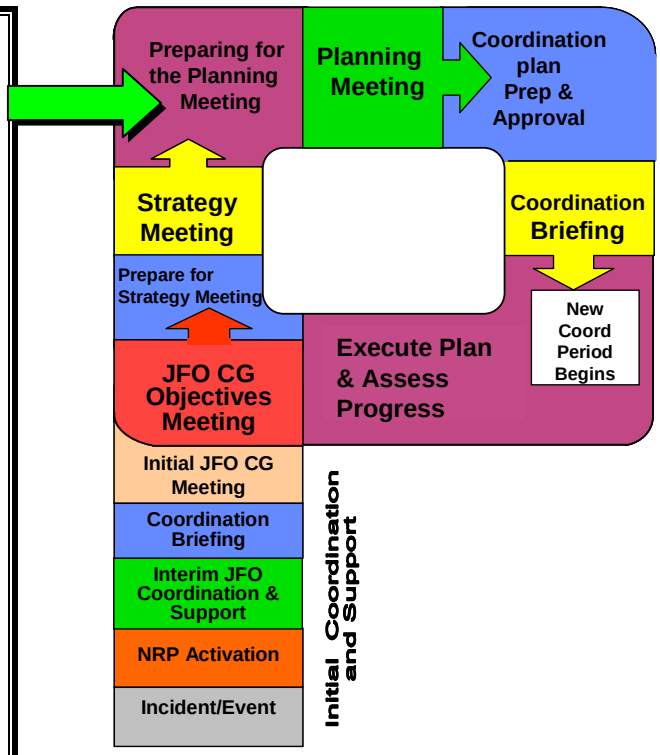
JFO CG:
- ❑ Provide guidance/clarification.
- ❑ Monitor ongoing strategic execution (progress in "operationalizing").

JFO OSC:
- ❑ Continue current-period Coordination and Support.
- ❑ Prepare for Planning Meeting.

JFO PSC:
- ❑ Facilitate JFO Coord staff and attendees' preparations for Planning Meeting.
- ❑ Publish/distribute meeting schedule and ensure attendees know roles.
- ❑ Allow no surprises.

JFO LSC:
- ❑ Prepare for Planning Meeting.
- ❑ Verify support requirements.

JFO FSC:
- ❑ Prepare for Planning Meeting.
- ❑ Verify financial and administrative requirements.



2.2.5 Planning Meeting

This meeting defines coordination and support objectives, strategies (both wide-area operations and incident support), and resource needs (both JFO internal and on-scene support) for the **next** coordination period. Depending on incident complexity, this meeting may require some time to explain the strategy fully to the JFO Staff. This meeting fine-tunes objectives and priorities, identifies and solves "alibi" problems, and defines work assignments and responsibilities on a JFO task tracking tool or completed ICS Form 215 (Operations Planning Worksheet). Displays in the meeting room should include objectives for the next coordination period, large sketch maps or charts clearly dated and timed (again, focused on wide-area operations, not on-scene incident tactics), a poster-sized ICS Form 215 for JFO-internal resource needs (such as technical specialists, etc.), a large support resource needs summary (based on the resource tracking tool in place at the JFO), a current consolidated resource inventory prepared by the Resource Unit, and current consolidated situation status displays prepared by the Situation Unit.

After the meeting, ICS Form 215 (when used) and the support resource needs tracking summary are used by the JFO Logistics Section Chief to prepare the national-level logistical resource orders, and used by the JFO Planning Section Chief to develop Coordination Plan assignment lists.

When: After the JFO Coordination Group Objectives and Strategy Meetings
Facilitator: JFO PSC
Attendees: Determined by JFO Coordination Group, generally JFO Coordination Group, JFO Coordination Staff, JFO Section Staff, Air Operations Branch Director, the JFO RUL, JFO Safety Coordinator, and Technical Specialists, as required.

General Tasks

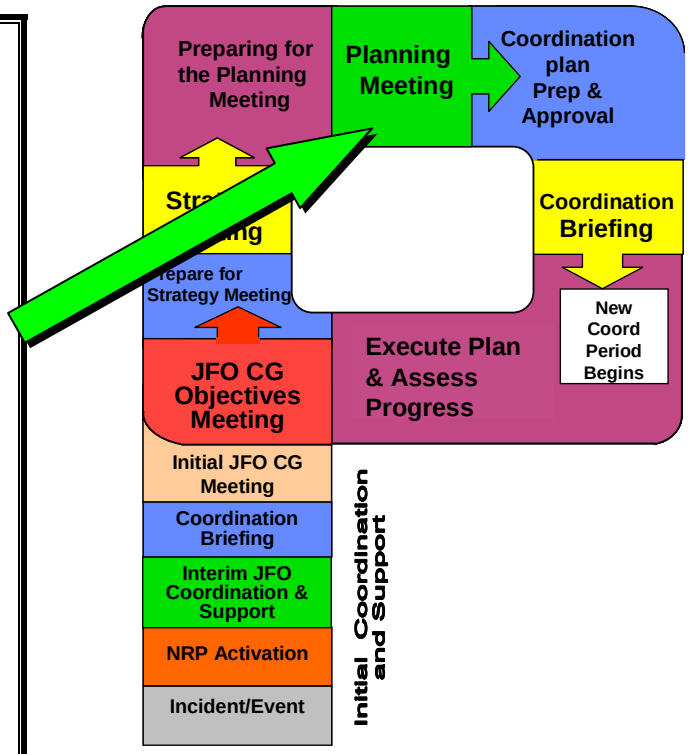
JFO CG:
- Provide appropriate leadership.
- Brief coordination and support objectives.

JFO OSC:
- Brief coordination and support strategies using support resource needs summary, ICS-215, maps, charts, etc.
- Brief JFO branch/group functions and jurisdictions.

JFO PSC:
- Facilitate Planning Meeting agenda.
- Brief present situation.
- Address/resolve coordination and support issues as needed, gain consensus.

JFO LSC:
- Brief logistical support and resource ordering status.

JFO FSC:
- Brief administrative and financial status/projections, etc.



Agenda Item		Primary Responsibility
1.	State incident objectives and policy issues.	JFO CG
2.	Brief consolidated situation, critical and sensitive areas, weather/sea forecast, and resource status/availability.	JFO Situation Unit Leader (SUL)
3.	Brief consolidated agency and Incident Commander objectives and strategies, noting gaps, overlaps, and seams.	JFO PSC
4.	State primary and alternative strategies to meet objectives.	JFO OSC
5.	Designate branch and group boundaries and functions as appropriate, use maps, support resource needs summary, and ICS Form 215.	JFO OSC
6.	Specify strategies for each branch and division, note limitations.	JFO OSC
7.	Specify resource strategies by divisions/groups.	JFO OSC
8.	Specify operations facilities and reporting locations and plot on map.	JFO OSC/ LSC
9.	Develop resources, support, and overhead order(s), both internal and support.	JFO LSC
10.	Consider support: communications, traffic, safety, medical, etc.	JFO LSC
11.	Consider safety considerations regarding Coordination Plan.	JFO Safety Officer (SO)
12.	Consider media considerations regarding Coordination Plan.	JFO Information Officer (IO)
13.	Report on expenditures and claims.	JFO FSC
14.	Finalize and approve work plan for the next coordination period.	JFO CG

2.2.6 Coordination Plan Preparation

Attendees immediately prepare their assignments for the Coordination Plan to meet the JFO Planning Section Chief deadline for assembling the Coordination Plan components. The deadline will be early enough to permit timely JFO Coordination Group approval and duplication of sufficient copies for the Coordination Briefing and for overhead. Note that due to the potentially large number of coordinating agencies in the JFO Coordination Group, the Coordination Plan cover must allow for concurrent signatures, and management of the JFO Coordination Group must assure necessary signatories will be present. Whenever possible, the PFO/FCO/FRC must agree with the JFO Coordination Group early in the process on which members will be Coordination Plan signatories.

When: Immediately following the Planning Meeting, the JFO PSC assigns the deadline.

Facilitator: JFO PSC

General Tasks

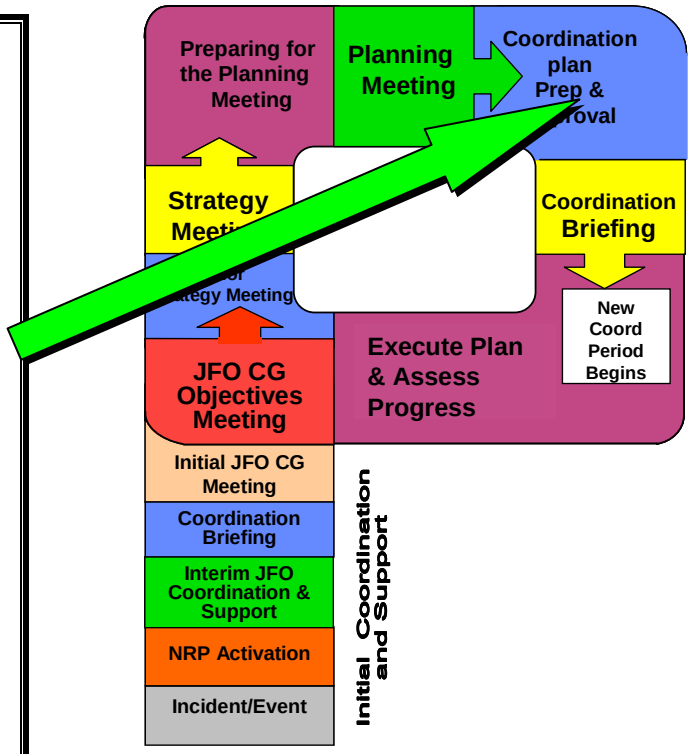
JFO CG:
- ❑ Review, approve, and sign the plan.

JFO OSC:
- ❑ Provide required information for inclusion into Coordination Plan.
- ❑ Communicate coordination and support status changes.

JFO PSC:
- ❑ Facilitate JFO Staff's Coordination Plan input.
- ❑ Ensure assignments and expectations are clear.
- ❑ Provide completed Coordination Plan to JFO CG for review/approval.
- ❑ Print and distribute completed Coordination Plan.

JFO LSC:
- ❑ Provide logistics information for Coordination Plan.
- ❑ Verify resources ordered.

JFO FSC
- ❑ Verify financial and administrative requirements for Coordination Plan.



Common Components	Primary Responsibility
1. Incident Objectives (ICS Form 202 or equivalent)	JFO Resources Unit
2. Organization List/Chart (ICS Forms 203/207 or equivalent)	JFO Resources Unit
3. Assignment List (ICS Form 204 or equivalent)	JFO Operations Section
4. Information-Sharing Procedures	JFO Situation Unit
5. Incident Map	JFO Situation Unit
6. Safety Plan	JFO Safety Coordinator

2.2.7 Coordination Meeting

This short meeting presents the Coordination Plan to the oncoming shift of the JFO organization. After this meeting, off-going supervisors should be interviewed by their relief and by the JFO Operations Section Chief in order to further confirm or adjust the course of the oncoming shift's Coordination Plan. Branch/Group supervisors may initiate shifts in strategy regarding matters that fall within their respective purviews. Similarly, a supervisor may reallocate resources within that division to adapt to changing conditions.

When: About an hour prior to each shift change
Facilitator: JFO PSC
Attendees: JFO Coordination Group, Coordination Staff, Branch Directors, Group Supervisors, Unit Leaders, others as appropriate.

General Tasks

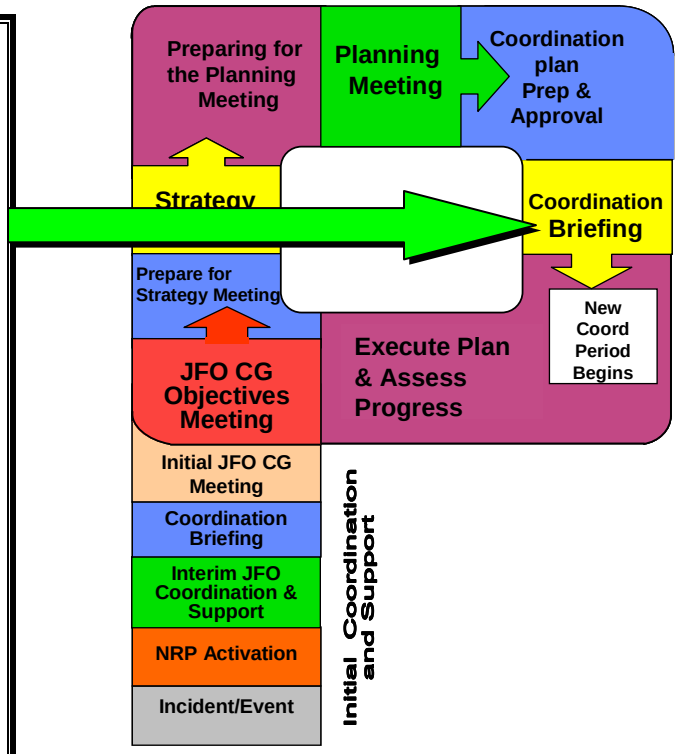
JFO CG:
- Provide guidance/clarification.
- Provide leadership presence.

JFO OSC:
- Provide Coordination Briefing for next coordination period.
- Ensure ICS-204 or equivalent tasking is clear.

JFO PSC:
- Facilitate Coordination Staff and attendees briefing responsibilities.
- Resolve questions.

JFO LSC:
- Brief transportation, communication, and supply issues.

JFO FSC:
- Brief administrative issues and provide financial report.



Agenda Item	Primary Responsibility
1. Review JFO Coordination Group objectives and changes to Coordination Plan.	JFO PSC
2. Discuss current strategy and last shift's "operationalizing" progress.	JFO OSC
3. Review forecast/expected situation in next period.	JFO SUL
4. Branch/Group and Air Operations assignment.	JFO OSC
5. Transport, communications, and supply updates.	JFO LSC
6. Safety message.	JFO SO

2.2.8 Assess Progress. Following the coordination brief, all Section Chiefs will review coordination and support strategy progress and make recommendations to the JFO Coordination Group in preparation for the next JFO Coordination Group Objective Meeting for the next coordination period. This feedback/information is gathered from various sources, including field observers, responder debriefs, stakeholders, etc.

General Tasks

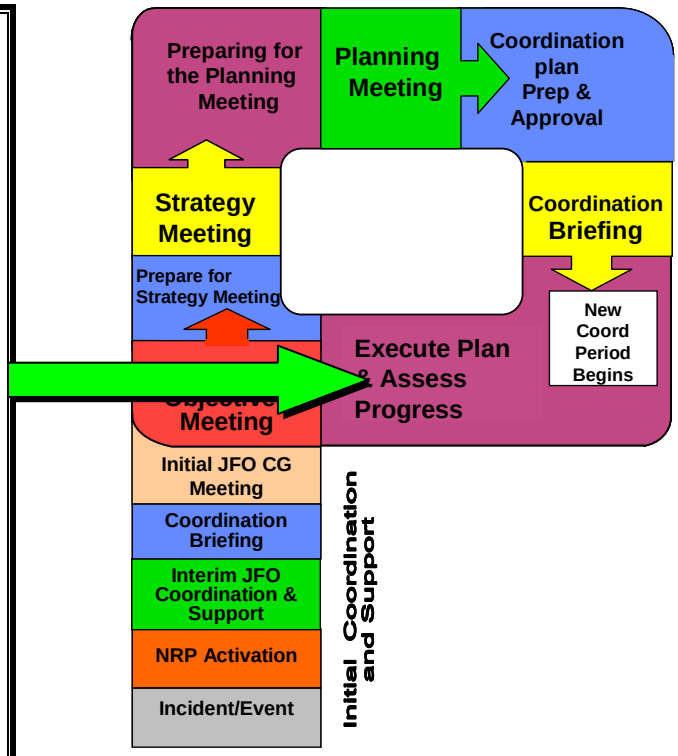
JFO CG:
- Monitor ongoing strategic implementation and support.
- Measure progress against stated objectives.
- Consider all national interest areas.

JFO OSC:
- Monitor ongoing strategic execution and make strategic changes as necessary.
- Measure/ensure progress against stated objectives.

JFO PSC:
- Facilitate Coordination Staff's effectiveness and efficiency as appropriate.
- Provide response objectives recommendations to JFO CG.

JFO LSC:
- Verify resources, resolve logistical problems.

JFO FSC:
- Facilitate smooth administrative and financial reporting.



2.3 Special Purpose Meetings.

The Special Purpose Meetings are most applicable to larger coordination and support efforts requiring a robust Coordination and Support Cycle, but may be useful during Initial Coordination, Support, and Assessment.

2.3.1 JFO Coordination Staff Meeting

Coordinate JFO Coordination Staff functions, responsibilities, and objectives. It is held before the Strategy Meeting, and JFO Coordination Staff (JFO Coordination Group, Chief of Staff, External Affairs, Office of the Inspector General, Defense Coordinating Officer, JFO Section Chiefs, JFO Legal Affairs Officer, and JFO External Affairs Officer) attend.

2.3.2 Coordination and Section Staff Meeting

This meeting provides an opportunity for the JFO Coordination and Section staffs (i.e., the Section Chiefs) to gather under informal conditions (breakfast/dinner) to discuss developing issues.

2.3.3 Business Management Meeting

This short meeting develops and updates the strategic plan for JFO-internal finance and logistical support. The agenda could include: documentation issues, cost sharing, cost analysis, finance requirements, resource procurement, and financial summary data. Attendees include: JFO Finance/Administration Section Chief, JFO Cost Unit Leader, JFO Logistics Section Chief, JFO Situation Unit Leader, and JFO Documentation Unit Leader.

2.3.4 News Briefing

This meeting briefs media and the public on the most current and accurate facts. It is set up by the External Affairs Officer, moderated by a JFO Coordination Group spokesperson (usually the External Affairs Officer), and features selected spokespersons. This briefing must be held away from the JFO. Spokespersons should be prepared by the External Affairs Officer to address anticipated issues. The briefing should be well planned, organized, and scheduled to meet the media's needs.

Tab 1 to Annex C: Decisionmaking Process

STEPS	DESCRIPTION	REMARKS
1. Understanding the Situation	☐ Identify and frame the mission • Incident/Issue/Threat • Scope of operation (e.g., number of people, geographic area) • Use of available time ☐ Conduct initial rapid assessment ☐ Determine if the threat is credible ☐ Alert Department Leadership Team and Staff personnel ☐ Develop mission statement ☐ Issue initial guidance	• *Develop framing questions to do mission analysis or make assumptions* • *Here is what we know* • *Here is what we don't know*
2. Establishing Objectives	☐ Analyze the initial guidance and intent ☐ Analyze Information/Intelligence preparation of the situation ☐ Develop Critical Success Factors (CSF) ☐ Develop strategic objectives • Source and macro-level purpose of mission or task • Critical planning factors/information requirements • Key integration issues ☐ Conduct detailed Situation Analysis • Desired end state/strategic intent • Specified-implied-essential tasks • Restraints/constraints • Available assets, their status, shortfalls • Assumptions ☐ Conduct risk assessment ☐ Develop Concept of the Operation (Macro) • Review facts and assumptions • OPSEC considerations • Interoperability – interagency collaboration and coordination ☐ Determine Public Affairs/Perception Management Requirements ☐ Finalize [*leadership*] mission statement, CSF and Objectives (intent on how to proceed) ☐ Conduct mission objectives and analysis brief ☐ Issue [*leadership's*] guidance	• *What must we do to have a perceived successful response* • *What are those things we need to do to be successful* • *Identify mission gaps* • *Framing the mission to convey success* • *Setting objectives and strategies that drives resources and tactics*

STEPS	DESCRIPTION	REMARKS
3. Develop and Generate Options	☐ Generate and develop options • Must be: Suitable, Feasible, Acceptable, Distinguishable, and Complete • Describes: Who, What, When, Where, Why and How? • Array of initial resources • List friendly elements and capabilities • List assumptions, known critical events and decision points ☐ Determine evaluation criteria ☐ Provide pros and cons for each option ☐ Analyze options and record the following • Actions—reactions—counteractions • Assets required • Timing of critical events/phasing • Critical Information Requirements • Control/direction measures • Synchronization/coordination/collaboration measures • Evaluation the advantages and disadvantages from each agency's relevant perspective ☐ Refine, modify, or eliminate options ☐ Determine tasks for DHS and other elements ☐ Rank order options in order of preference (minimum of two no more that three options available) and capture rational ☐ Determine risk/mitigation measures ☐ Prepare leadership brief on recommended options	• *Possible use of predetermined mission area groups (e.g., Law Enforcement, Public Health, Maritime Security, Border Security, Transportation Security) or sector objectives* • *COA meets collective incident objective addressing existing constraints* • *Maximizing agency objectives while meeting collective incident objectives* • *Consensus that best meets incident objectives* • *Prudent branches and sequels*
4. Approval and Disseminate	☐ Conduct the option comparison/decision brief for leadership ☐ Leadership approves a recommended or modified option ☐ Leadership approves a final intent statement and the Critical Information Requirements to support the selected options ☐ Produce and disseminate direction/guidance as needed for plan refinement, orders preparation, rehearsal, and execution	

STEPS	DESCRIPTION	REMARKS
5. Execute and Assess	☐ Monitor situation, revise and update options as required	

NOTES:

- Take the worst-case scenario in shortest amount of time (1 hour) to have a decision (COA) ready and then work backwards with more time – must work at national level with macro view as well as local (tactical) level.
- Problem is getting a consensus of competing agendas among the different agencies.

Tab 2 to Annex C: CP Cover Sheet

1. Incident of National Significance Name	2. Coordination Period covered by Plan (Date/Time) From: To:	Coordination Plan COVER SHEET

3. Approved by the JFO Coordination Group:

ORG	NAME	ORG	NAME

COORDINATION PLAN

The items checked below are included in this Coordination Plan:

☐ ICS 202-JFO (Coordination and Support Objectives)

☐ ICS 204-JFOs (Assignment Lists)
One Copy each of any ICS 204-JFO attachments:

☐ ICS 205-JFO (Information Sharing Procedures)

☐ ICS 209-JFO (Situation Briefing)

Other Attachments

☐ _____

☐ _____

☐ _____

☐ _____

☐ _____

4. Prepared by: **Date/Time**

Tab 3 to Annex C: Coordination Objectives

1. Incident of National Significance Name	2. Coordination Period (Date/Time) From: To:	**COORDINATION OBJECTIVES ICS 202-JFO**

3. Coordination and Support Objective(s)

4. Coordination Period Command Emphasis (Safety Message, Priorities, Key Decisions/Directions)

Approved Site Safety Plan Located at:

5. Prepared by: (JFO Planning Section Chief) **Date/Time**

Tab 4 to Annex C: Assignment List

1. Incident Name	2. Coordination Period (Date/Time) From: To:	Assignment List ICS 204-JFO
3. Branch	4. Group/Staging	

5. Operations Personnel Name Affiliation Contact # (s)

JFO Operations Section Chief: _____

Branch Director: _____

Group Supervisor: _____

6. Resources Assigned "X" indicates 204a attachment with additional instructions

Resource Identifier	Leader	Contact Info. #	# of Persons	Reporting Info/Notes/Remarks	
					☐
					☐
					☐
					☐
					☐
					☐
					☐
					☐
					☐

7. Work Assignments

8. Special Instructions

9. Communications (radio and/or phone contact numbers needed for this assignment)

Name/Function Radio: Freq./System/Channel Phone Cell/Pager _____

_____ _____ _____ _____ _____

_____ _____ _____ _____ _____

_____ _____ _____ _____ _____

Emergency Communications

Medical _____ Evacuation _____ Other _____

10. Prepared by Date/Time	11. Reviewed by (JFO PSC) Date/Time	12. Reviewed by (JFO OSC) Date/Time

Tab 5 to Annex C: Assignment List Attachment

1. Incident Name	2. Coordination Period (Date/Time) From: To:	ASSIGNMENT LIST ATTACHMENT ICS 204a-JFO
3. Branch	4. Group	
5. Specific Resource (if any)	6. Leader	7. Assignment Location

8. Work Assignment Special Instructions, Special Equipment/Supplies Needed for Assignment, Special Environmental Considerations, Special Site Specific Safety Considerations

Approved Site Safety Plan Located at:

9. Other Attachments (as needed)

☐ **Map/Chart** ☐ **Weather Forecast/Tides/Currents** ☐ _____

☐ _____ ☐ _____ ☐ _____

10. Prepared by Date/Time	11. Reviewed by (JFO PSC) Date/Time	12. Reviewed by (JFO OSC) Date/Time

Tab 6 to Annex C: ICS-209-JFO, Coordination Status Summary

Document Security Classification

1. Incident Name	**2. Coordination Period (Date / Time)** From: To: Time of Report	**COORDINATION STATUS SUMMARY ICS 209-JFO** (Revised 1/05)

3. Type of Incident of National Significance

4. Incident Location

Map / Chart / Graphic / Picture **Text Description**

5. Time of Incident	Local Time & Zone	Comments:
Incident Occurred		
Initial Response		
IONS Declared		
IOF Established		
JFO Established		

6. Weather Conditions

Current Conditions:	Extended Forecast:
Comments:	

7. Projected Effect of Weather on On-Scene Status & Capabilities

Classified or Sensitive Security Information Statement:

Document Security Classification

8. Threats and Causal Factors

9. Safety Status/Personnel Casualty Summary

	Since Last Report	Adjustments To Previous Coordination Period	Incident Total
Responder Injury			
Responder Death			
Public Missing (Active Search)			
Public Missing (Presumed Lost)			
Public Uninjured			
Public Injured			
Public Dead			
Total Public Involved			

Comments:

10. Evacuation Status

	Since Last Report	Adjustments To Previous Coordination Period	Incident Total
Total to be Evacuated			
Number Evacuated			

Comments:

11. Property Damage Summary

Property Type	Damage Estimate
	$
	$
	$
	$
	$
	$
	$
	$
	$
	$

Comments:

Classified or Sensitive Security Information Statement:

Document Security Classification

12. Affected Infrastructure Summary

Infrastructure	Extent of involvement

Comments:

13. Terrorism Nexus

14. General Population Status Summary

	Since Last Report	Adjustments To Previous Coordination Period	Incident Total
Total Public Potentially Involved			
Public Currently At Risk			
Public Projected At Risk			
Public Isolated (safe)			
Total Public Currently Involved			
Public Missing			
Public Dead and Injured			
Public Under Treatment			
Public Safe Uninjured			

Comments:

15. Extent of Contamination

Classified or Sensitive Security Information Statement:

Document Security Classification

16. On-Scene Capabilities (not assets)

Capability	Since Last Report	Adjustments To Previous Coordination Period	Incident Total

Comments:

17. On-Scene En-route to Scene (not assets)

Capability	Since Last Report	Adjustments To Previous Coordination Period	Incident Total

Comments:

18. Requests for Additional On-Scene Support

Tracking #	Status	Support Request	Discussion

Comments:

Classified or Sensitive Security Information Statement:

Document Security Classification

19. Possible Cascading Effects of On-scene Situation

20. Possible WMD Effects from On-scene Situation

21. Indications On-scene of Possible Follow-on Incidents

22. Summary of Coordinating Federal, State, and Local OPCENS & Agencies

Federal OPCENs / Agencies	*State OPCENs / Agencies*	*Local OPCENs / Agencies*

Comments:

Classified or Sensitive Security Information Statement:

Document Security Classification		
23. Summary of Coordinated Wide-Area Objectives		
Coordinating Federal Agencies	***Coordinating State Agencies***	***Coordinating Local Agencies***
Comments:		
24. Summary of Coordinated Wide-Area Strategies		
Coordinating Federal Agencies	***Coordinating State Agencies***	***Coordinating Local Agencies***
Comments:		
Classified or Sensitive Security Information Statement:		

Document Security Classification					
25. Significant or Noteworthy Response Assets / Resources On Scene (See attached IAPs for incident details)					
Kind	Notes	# Ordered	# Available	# Assigned	# Out of Service
Comments:					
Classified or Sensitive Security Information Statement:					

Document Security Classification		
26. Federal/State/Local/International/Private Sector Contacts Made		
Date	**Contact**	**Contact Notes**
27. COOP/COG Actions Anticipated		
28. National Capital Region Impacts Anticipated		
Classified or Sensitive Security Information Statement:		

Document Security Classification	
29. International Impacts Anticipated	
30. Special Notes and Other Considerations	
31. Prepared by:	**Date/Time Prepared:**
Classified or Sensitive Security Information Statement:	

Annex D: Logistical Requirements

1.0 Joint Field Office Logistics Requirements (conceptual)

Joint Field Office Component	Magnitude of JFO Activation		
	Type III (small)	**Type II (medium)**	**Type I (large)**
PFO Support Staff	*15 persons* 3,000 ft^2	*25 persons* 5,000 ft^2	*35 persons* 7,000 ft^2
JFO Coordination Group	*6 persons* 1,200 ft^2	*8 persons* 1,600 ft^2	*10 persons* 2,000 ft^2
JFO Coordination Staff	*15 persons* 3,000 ft^2	*25 persons* 5,000 ft^2	*35 persons* 7,000 ft^2
JFO Joint Information Center (JIC)	*3 persons* 600 ft^2	*4 persons* 800 ft^2	*5 persons* 1,000 ft^2
Operations Section			
Response and Recovery Branch			
▪ Forward presence (only) for FEMA ERT-A	*6 persons* 1,200 ft^2	*12 persons* 2,400 ft^2	*40 persons* 8,000 ft^2
▪ Full onsite Human Services Group	*30 persons*	*150 persons*	*300 persons*
▪ Full onsite Emergency Services Group		*100 persons*	*200+ persons*
▪ Full onsite Infrastructure Support Group	*30 persons*	*100 persons*	*200+ persons*
▪ Full onsite Community Recovery and Mitigation Group	*6 persons*	*10 persons*	*20 persons*
Law Enforcement Investigative Operations Branch (FBI JOC)			
▪ Forward presence (only) for FBI JOC	*3 persons* 600 ft^2	*4 persons* 800 ft^2	*5 persons* 1,000 ft^2
▪ Full Branch onsite	*60 persons* 12,000 ft^2	*100 persons* 20,600 ft^2	*140 persons* 28,000 ft^2
▪ SCIF	*3 persons* 600 ft^2	*10 persons* 2,000 ft^2	*15 persons* 3,000 ft^2
Security Operations Branch (DHS/USSS MACC)			
▪ Forward presence (only) for USSS MACC	*3 persons* 600 ft^2	*4 persons* 800 ft^2	*5 persons* 1,000 ft^2
▪ Full Branch onsite	*60 persons* 12,000 ft^2	*100 persons* 20,000 ft^2	*140 persons* 28,000 ft^2
Intelligence Operations Branch	*10 persons* 2,000 ft^2	*50 persons* 10,000 ft^2	*70 persons* 14,000 ft^2

Joint Field Office Component	Magnitude of JFO Activation		
	Type III (small)	**Type II** (medium)	**Type I** (large)
Planning Section			
▪ Situation Unit	*2 persons* 400 ft^2	*4 persons* 800 ft^2	*5 persons* 1,000 ft^2
▪ GIS Unit	*2 persons* 400 ft^2	*4 persons* 800 ft^2	*5 persons* 1,000 ft^2
▪ Resource Unit	*2 persons* 400 ft^2	*4 persons* 800 ft^2	*5 persons* 1,000 ft^2
▪ Documentation Unit	*2 persons* 400 ft^2	*4 persons* 800 ft^2	*5 persons* 1,000 ft^2
▪ Intelligence Unit (if activated)	*2 persons* 400 ft^2	*4 persons* 800 ft^2	*5 persons* 1,000 ft^2
▪ Demobilization Unit	*2 persons* 400 ft^2	*4 persons* 800 ft^2	*5 persons* 1,000 ft^2
▪ Scientific Unit	*4 persons* 800 ft^2	*7 persons* 1,400 ft^2	*10 persons* 2,000 ft^2
Logistics Section			
▪ Coordination and Planning Branch	*2 persons* 400 ft^2	*8 persons* 1600 ft^2	*10 persons* 2,000 ft^2
▪ Resource Management Branch	*2 persons* 400 ft^2	*4 persons* 800 ft^2	*5 persons* 1,000 ft^2
▪ Support Branch	*3 persons* 600 ft^2	*5 persons* 1000 ft^2	*8 persons* 1,600 ft^2
▪ Service Branch	*4 persons* 800 ft^2	*7 persons* 1,400 ft^2	*10 persons* 2,000 ft^2
Finance/Administration Section			
▪ Time Unit	*2 persons* 400 ft^2	*7 persons* 1,400 ft^2	*10 persons* 2,000 ft^2
▪ Procurement Unit	*2 persons* 400 ft^2	*7 persons* 1,400 ft^2	*10 persons* 2,000 ft^2
▪ Cost Unit	*2 persons* 400 ft^2	*7 persons* 1,400 ft^2	*10 persons* 2,000 ft^2.
▪ Compensation/Claims Unit	*2 persons* 400 ft^2	*7 persons* 1,400 ft^2	*10 persons* 2,000 ft^2.

Notes

1. Numbers of staff will be incident-dependent from one type of incident to another. These are baseline numbers by program area and could reflect one or all program areas represented at the same time.
2. Reflects steady-state operations once the facility is fully operational. Initial surge staff numbers would be significantly higher for the setup of the facility. If not deployed in support of higher priority missions, MERS deployments would typically include 13 for a Type III, 20 for a Type II, and 25+ for Type I depending on the complexity of the operation being supported and the infrastructure build-out.

Scalability of the Joint Field Office

The JFO uses the scalable organizational structure of the NIMS ICS in the context of both pre-incident and post-incident management activities. The JFO organization and physical layout adapt to the magnitude and complexity of the situation at hand. As discussed in the National Response Plan's Concept of Operations, the typical JFO organization is defined below for the

following scenarios:

1) Type I (Major) **Disaster**, no security or investigative activation.
2) Type II **Heightened Threat** of Terrorism, no credible threat of WMD
3) Type I **Heightened Threat** of Terrorism, credible threat of WMD
4) Type I **Federal-to-Federal** Support (Spill of National Significance)
5) Type III **Federal-to-Federal** Support (Chemical Release Accident)

2.0 Scenario One: Type I (Major) Disaster

[RESERVED]

Joint Field Office Component	Activation Size	Size Requirements
PFO Support Staff	NONE	
JFO Coordination Group	SMALL	
JFO Coordination Staff	NONE	
JFO Joint Information Center (JIC)	MEDIUM	
Operations Section		
Response and Recovery Branch	LARGE	
▪ Human Services Group	LARGE	
▪ Emergency Services Group	LARGE	
▪ Infrastructure Support Group	LARGE	
▪ Community Recovery and Mitigation Group	LARGE	
Law Enforcement Investigative Operations Branch	NONE	
Security Operations Branch	NONE	
Intelligence Operations Branch	NONE	
Planning Section		
▪ Situation Unit	LARGE	
▪ GIS Unit	LARGE	
▪ Resources Unit	LARGE	
▪ Documentation Unit	MEDIUM	
▪ Intelligence Unit (if activated)	NONE	
▪ Demobilization Unit	SMALL	
▪ Scientific Unit	SMALL	
Logistics Section		
▪ Coordination and Planning Branch	LARGE	
▪ Resource Management Branch	LARGE	
▪ Supply Branch	LARGE	
▪ Information Services Branch	LARGE	
Finance / Administration Section		
▪ Time Unit	LARGE	
▪ Procurement Unit	LARGE	
▪ Cost Unit	LARGE	
▪ Compensation/Claims Unit	MEDIUM	
Total Logistical Footprint		*X persons* X ft^2

3.0 Scenario Two: Type II Heightened Threat of Terrorism w/out WMD

[RESERVED]

Joint Field Office Component	Activation Size	Size Requirements
PFO Support Staff	MEDIUM	
JFO Coordination Group	MEDIUM	
JFO Coordination Staff	SMALL	
JFO Joint Information Center (JIC)	SMALL	
Operations Section		
Response and Recovery Branch		
▪ Forward Presence (only)	LARGE	
Law Enforcement Investigative Operations Branch		
▪ Full Branch onsite	LARGE	
▪ SCIF	LARGE	
Security Operations Branch (MACC)		
▪ Full Branch onsite	LARGE	
Intelligence Operations Branch (IOC)	SMALL	
Planning Section		
▪ Situation Unit	LARGE	
▪ GIS Unit	LARGE	
▪ Resource Unit	SMALL	
▪ Documentation Unit	MEDIUM	
▪ Intelligence Unit (if activated)	NONE	
▪ Demobilization Unit	LARGE	
▪ Scientific Unit	LARGE	
Logistics Section		
▪ Coordination and Planning Branch	SMALL	
▪ Resource Management Branch	SMALL	
▪ Supply Branch	SMALL	
▪ Information Services Branch	SMALL	
Finance / Administration Section		
▪ Time Unit	SMALL	
▪ Procurement Unit	SMALL	
▪ Cost Unit	SMALL	
▪ Compensation / Claims Unit	NONE	
Total Logistical Footprint		*XXX persons* XX ft^2

4.0 Scenario Three: Type I Heightened Threat of Terrorism w/ WMD

[RESERVED]

Joint Field Office Component	Activation Size	Size Requirements
PFO Support Staff	MEDIUM	
JFO Coordination Group	MEDIUM	
JFO Coordination Staff	SMALL	
JFO Joint Information Center (JIC)	SMALL	
Operations Section		
Response and Recovery Branch		
▪ Forward Presence (only)	LARGE	
Law Enforcement Investigative Operations Branch		
▪ Full Branch onsite	LARGE	
▪ SCIF	LARGE	
Security Operations Branch (MACC)		
▪ Full Branch onsite	LARGE	
Intelligence Operations Branch (IOC)	SMALL	
Planning Section		
▪ Situation Unit	LARGE	
▪ GIS Unit	LARGE	
▪ Resource Unit	SMALL	
▪ Documentation Unit	MEDIUM	
▪ Intelligence Unit (if activated)	NONE	
▪ Demobilization Unit	LARGE	
▪ Scientific Unit	LARGE	
Logistics Section		
▪ Coordination and Planning Branch	SMALL	
▪ Resource Management Branch	SMALL	
▪ Supply Branch	SMALL	
▪ Information Services Branch	SMALL	
Finance / Administration Section		
▪ Time Unit	SMALL	
▪ Procurement Unit	SMALL	
▪ Cost Unit	SMALL	
▪ Compensation / Claims Unit	NONE	
Total Logistical Footprint		*XXX persons* XX ft^2

5.0 Scenario Four: Type I Federal-to-Federal Support (Spill of National Significance)

[RESERVED]

Joint Field Office Component	Activation Size	Size Requirements
PFO Support Staff		
JFO Coordination Group		
JFO Coordination Staff		
JFO Joint Information Center (JIC)		
Operations Section		
Response and Recovery Branch		
▪ Forward Presence (only)		
Law Enforcement Investigative Operations Branch		
▪ Full Branch onsite		
▪ SCIF		
Security Operations Branch (MACC)		
▪ Full Branch onsite		
Intelligence Operations Branch (IOB)		
Planning Section		
▪ Situation Unit		
▪ GIS Unit		
▪ Resource Unit		
▪ Documentation Unit		
▪ Intelligence Unit (* if activated)		
▪ Demobilization Unit		
▪ Scientific Unit		
Logistics Section		
▪ Coordination and Planning Branch		
▪ Resource Management Branch		
▪ Supply Branch		
▪ Information Services Branch		
Finance / Administration Section		
▪ Time Unit		
▪ Procurement Unit		
▪ Cost Unit		
▪ Compensation / Claims Unit		
Total Logistical Footprint		*XXX persons* XX ft^2

6.0 Scenario Five: Type III Federal-to-Federal Support (Chemical Release Accident)

[RESERVED]

Joint Field Office Component	Activation Size	Size Requirements
PFO Support Staff		
JFO Coordination Group		
JFO Coordination Staff		
JFO Joint Information Center (JIC)		
Operations Section		
Response and Recovery Branch		
▪ Forward Presence (only)		
Law Enforcement Investigative Operations Branch		
▪ Full Branch onsite		
▪ SCIF		
Security Operations Branch (MACC)		
▪ Full Branch onsite		
Intelligence Operations Branch (IOB)		
Planning Section		
▪ Situation Unit		
▪ GIS Unit		
▪ Resource Unit		
▪ Documentation Unit		
▪ Intelligence Unit (if activated)		
▪ Demobilization Unit		
▪ Scientific Unit		
Logistics Section		
▪ Coordination and Planning Branch		
▪ Resource Management Branch		
▪ Supply Branch		
▪ Information Services Branch		
Finance / Administration Section		
▪ Time Unit		
▪ Procurement Unit		
▪ Cost Unit		
▪ Compensation / Claims Unit		
Total Logistical Footprint		*XXX persons* XX ft^2

7.0 JFO Size Requirements Estimation Worksheet

[RESERVED]

Joint Field Office Component	Magnitude of JFO Activation		
	Size (Small /Medium /Large)	**Number of People**	**Size Required**
PFO Support Staff			
JFO Coordination Group			
JFO Coordination Staff			
JFO Joint Information Center (JIC)			
Operations Section			
Response and Recovery Branch			
▪ Forward presence (only) for FEMA ERT-A			
▪ Full onsite Human Services Group			
▪ Full onsite Emergency Services Group			
▪ Full onsite Infrastructure Support Group			
▪ Full onsite Community Recovery and Mitigation Group			
Law Enforcement Investigative Operations Branch (FBI JOC)			
▪ Forward presence (only) for FBI JOC			
▪ Full Branch onsite			
▪ SCIF			
Security Operations Branch (DHS/USSS MACC)			
▪ Forward presence (only) for USSS MACC			
▪ Full Branch onsite			
Intelligence Operations Branch			
Planning Section			
▪ Situation Unit			
▪ GIS Unit			
▪ Resource Unit			
▪ Documentation Unit			
▪ Intelligence Unit (if activated)			
▪ Demobilization Unit			
▪ Scientific Unit			
Logistics Section			
▪ Coordination and Planning Branch			
▪ Resource Management Branch			
▪ Supply Branch			
▪ Information Services Branch			
Finance / Administration Section			
▪ Time Unit			
▪ Procurement Unit			
▪ Cost Unit			
▪ Compensation / Claims Unit			
Total Logistical Footprint: (baseline estimate)			

Tab 1 to Annex D: Pre-deployment Conference Call Checklist

The Pre-deployment Conference Call will be initiated by the Senior Disaster Logistics Official and conducted as soon as possible and should include at a minimum the following participants:

- JFO Coordination Group
- Federal Coordinating Officer (FCO) or Representative
- Logistics Section Chief
- Information Technology Coordinator
- Readiness, Response, and Recovery (RRR), Mobile Operations Branch RR (MOB)
- Supporting Mobile Emergency Response Support (MERS) Detachment
- RRR, Operations Center Branch
- Information Technology Services Directorate, Engineering Division
- Information Technology Services Directorate, Disaster Response Branch
- ITSD, Program Management Group
- National HELP Desk
- Disaster Information Clearinghouse (DISC)
- FEMA Logistics Center
- OSD, Program Services Division (OS-PS)/Mail Management
- OSD, Security Division
- Safety Coordinator
- NEMIS Ops

Tab 2 to Annex D: PFO Go Kit Footprint

The DHS Office of Operations IMD has assembled PFO support "go kits" that will be strategically placed in eight regional areas and the National Capital Region. These kits afford instant connectivity once installed with appropriate security safeguards, without regard to agency firewalls and/or the operating location of the cell. Each kit has appropriate equipment to serve 12 PFO support staff members. DHS/ Office of Operations IMD will maintain and, when appropriate, move kits to the location of the PFO support staff. The NCR Go Kit can also be used as portable system for the IIMG and/or the DHS/ Office of Operations IMD in the event that COOP locations, IIMG, or Office of Operations IMD facilities are not operational.

The "kits" consist of the following:

Quantity	Item	Description
12	Latitude D600 Notebooks	Intel Pentium 4 M (1.8Ghz) 14" SXVGA+ Display; Windows XP Pro w/SP1; Office XP 1024Mb RAM; 40Gb Hard Drive MiniPCI Wireless Card; Dell Logitech, Mouse (USB); Internal 56K Modem; 8-24-24-24X; WDVD/CDRW Combo Drive 90W AC Adapter; Mouse Pad 6 Cell Primary Battery; 128Mb USB Flash Storage Drive (Thumb Drive); 3-Year Limited Warranty plus 3-Year Next Business Day Onsite Service
12	Network Cables	Cat 5e 20 Feet
1	Switch	Netgear JFS524 2 "16 port switch"
2	Printer	Hewlett Packard 5510 All-in-one Printer
16	Power Strips	6 Outlet w/ 15ft Cord
10	Secure Cell Phones	PFO, Deputy PFO, COS, OSC Officer, PAO, HSOC Rep
12	JRIES	JRIES Software (Gov't owned)
1	SIPRNET	HSIN/HSDN (SECRET) hardware for portable connectivity. There are 16 of these available at DHS HQS. One of these must be reserved for each PFO support staff in the interim.
2	STE's	Secret Level
1	FAX	Secure with copy capability
12	Protective Masks	Quick2000 short-term protective mask with hood; Quick2000 training mask with hood; soft carrying case item 600665
N/A	Admin Package	Hard Side shipping lockers, admin supplies (pens, paper, files), flashlights, printer supplies, etc.

Tab 3 to Annex D: DHS/HSOC Go Kit Footprint

The DHS/HSOC maintains PFO support "go kits" with the following general capability footprint:

XX computers with the following capabilities:

- Microsoft Suite
- Internet Browser
- GIS Viewer (ArcView)
- GIS Thick Client Applications
- Java
- Active X
- CD/DVD Duplication software
- HSIN/JRIES
- LEO
- I-MAP
- Paging Software
- Operations Center Management Tools (e.g., E-Team, WebEOC, EM2000, DMIS)
- Commercial Imagery Production Application
- NEMIS
- IFMIS
- Adobe Acrobat

Annex E: Communications and Information Sharing

1.0 Purpose and Scope

This annex will describe procedures employed by the JFO for both intra-JFO information sharing and sharing between the JFO and other organizations. In keeping with the NRP and NIMS core concepts, all information flow processes will be structured to present the least amount of burden upon the local incident commander. To the greatest extent possible, ICS concepts will be applied.

Information flow and communications involving classified material will be governed by standard DHS information and operations security procedures.

Information flow and communications involving the Law Enforcement/Investigations Operations Branch (FBI/JOC) will be governed by FBI information and operations security procedures.

Public Information and Joint Information Center activities are outside the scope of this annex.

2.0 Intra-JFO Communications

2.1 HSIN-JFOnet

- The primary communication platform for JFO personnel to pass data, provide and obtain situational awareness, collaborate on report generation, and submit and receive RFIs will be the HSIN-JFOnet. JFOnet is a component of the DHS Homeland Security Information Network and is managed by the HSOC.
- HSIN-JFOnet is a web-based communications tool suite with Geospatial Intelligence Mapping, Real-Time Collaboration, Document Sharing, and Incident Tracking/Chronological Logging Tool. JFOnet operates at the sensitive but unclassified security classification level.
- JFOnet can operate as a free-standing local area network (LAN) for exclusive use within the JFO in the event of loss of connectivity to the public Internet.
- Provided external connectivity exists, other organizations such as HSOC, IIMG, State/local emergency management agencies, DHS components, and other appropriate Federal/State/local agencies may access JFOnet for passive situational awareness monitoring or active collaboration as needed.
- To optimize internal and external situational awareness, to the greatest extent possible, the JFO personnel will refrain from point-to-point e-mails and utilize the web-based JFOnet.
- The JFO's Logistics Section, Communications Unit, in tandem with HSOC personnel assigned to the JFO, shall manage JFOnet, including providing onsite assistance.

- Personnel assigned to the JFO will, upon check-in, be assigned account names and passwords and provided with user-friendly instruction cards describing how to use the system.

2.2 Information Flow

- ICS information management principles will be followed to the greatest extent possible. A basic ICS tenet is that information flows freely, but tasks and directions follow formal chains of command. The collaboration and posting functions of JFOnet facilitate adherence to this concept.
- When established within the JFO structure, the situation unit or documentation unit, at the Planning Section Chief's discretion, is responsible for receiving, consolidating, and preparing situation reports (SITREPS). (See Annex E for a sample.)
- All entities within the JFO, for SITREP inputs, will place their respective inputs onto the JFOnet for construction of the distributed SITREP.
- All JFO entities have a responsibility for posting spot reports (SPOTREPs) on JFOnet as information is received from their areas of responsibility as defined by ICS. (See Annex E for a sample.)
- The report cycle of issuance of SITREPS will be determined by the JFO Coordination Group, generally following the standard ICS practice of one SITREP being issued per operating period.

2.2.1 Information Intake

Information flows into the JFO at many points. This information will generally be routed as follows:

- General unclassified information. The JFO Situation Unit is the primary intake and assessment point for general unclassified information. Information may be routed in hard copy or by posting to the "Situation Unit Incoming" folder in JFO-net. In the case of a JFO established for a NSSE, the Security Operations Branch (MACC) will perform this function unless and Incident of National Significance occurs during the NSSE. Following assessment, the JFO Situation Unit or MACC (depending on the circumstance) posts the information to the information management system and will route the information to internal and external customers (including the JOC Intelligence Unit, Intelligence Operations Center or JFO Intelligence Section, and JFO Information and Intelligence Unit).
- Unclassified event-related security information. The MACC is the primary intake and assessment point for event-related security information. Where the MACC has not been established, the JFO Situation Unit becomes the primary point of entry for security or event-related unclassified information.
- Law enforcement restricted information. The JOC Intelligence Unit is the primary intake and assessment point for Law Enforcement Restricted Information. Information may be routed to the JOC Intelligence Unit in hard copy, by phone, or other method identified by the FBI. Where the JOC has not been established, the FBI Field Office becomes the primary intake and assessment point for Law Enforcement Restricted information. Information may be routed to the JFO

Information and Intelligence Unit by hard copy or by posting to the "LE Information Incoming" folder in HSIN.

- Classified intelligence information. The Intelligence Operations Center (IOC) or JFO Intelligence Branch (depending on the circumstance) is the primary intake and assessment point for classified intelligence information. Information may be routed to the IOC/JFO Intelligence Branch by hard copy, fax, phone, or by SIPRNET. Where the IOC/JFO Intelligence Branch has not been established, the JOC Intelligence Unit becomes the primary intake and assessment point for classified intelligence information. Where neither the IOC/JFO Intelligence Branch nor the JOC Intelligence Unit have been established, the JFO Information and Intelligence Unit becomes the primary intake and assessment point.

2.2.2 Internal Information Exchange

- Based on the JFO Information Sharing Procedures developed by the JFO Situation Unit (see Section 4.4.1 of the SOP), staff in the JFO Situation Unit, JFO Information and Intelligence Unit, JOC Intelligence Unit, MACC, and Intelligence Operations Center/JFO Intelligence Branch will forward information they believe relevant to another unit to that unit for review. This process is generally known as "cross-posting."
- Once information has been cross-posted, it will be treated as new information by the receiving customer (i.e., units will not be empowered to bypass another unit's information intake, tracking, and assessment processes). For this reason, originator information (including sources, POCs, date/time stamp, information confidence, and so on) should be included to the extent permissible by information security protocols.

2.2.3 Situation Report Development

- While the JFO Planning Section Chief may arrange duties within the Section as necessary for efficient functioning, the JFO Documentation Unit will normally distill information from the JFO Information Management System to comprise the "base" information for the many and various Situation Reports (SITREPs) required by any member of the JFO Coordination Group (see Annex E for a sample).
- All entities within the JFO will provide their respective inputs via JFOnet for construction of the distributed SITREP.
- All JFO entities have a responsibility for posting spot reports (SPOTREPS) on JFOnet as information is received from their areas of responsibility as defined by ICS (See Annex E for a sample).
- The report cycle of issuance of SITREPS will be determined by the JFO Coordination Group, generally following the standard ICS practice of one SITREP being issued per operating period.

2.3 Requests for Information (RFIs) Management (Exclusive of Intelligence-Related RFIs)

- RFIs made to the JFO from other organizations and internal RFIs will be routed to the JFO Planning Section Chief (PSC). The JFO PSC will ensure that the RFI is posted

onto JFOnet. Specific desks within the JFO may be tasked by the JFO PSC to provide information in response to the RFI.

- The JFO Situation Unit or Documentation Unit, at the JFO PSC's discretion, will coordinate RFI responses with the JFO Coordination Group.
- The JFO Situation Unit will maintain an RFI tracking log to eliminate duplicate taskings and track responses.

2.4 Specialized Management of Intelligence-Related RFIs

- Management and flow of intelligence-related RFIs will be dependent upon the organizational location of the Intelligence Component within the JFO structure. If a Law Enforcement/Investigations Operations Branch (FBI/JOC) is activated and the component is integrated into it, RFIs will be managed in accordance with the instructions of the Senior Federal Law Enforcement Official (SFLEO) as part of the JFO Coordination Group. If Intelligence is integrated into the Planning Section, the Section Chief, in coordination with the JFO Coordination Group, shall establish procedures and communicate them via JFOnet. If Intelligence is a separate section, the Intelligence Section Chief, in coordination with the JFO Coordination Group, shall establish procedures and communicate them via JFOnet.
- This specialized management shall apply to all intelligence-related RFIs regardless of the classification level.
- Handling procedures shall include appropriate information, communications, and operational security provisions based upon the classification of the material.

2.5 Resource Status Reporting

- [FEMA Disaster Resource Tracking Systems]
- The HSOC representative to the Resource Unit will cross-post relevant data from the DHS/FEMA Resource Tracking System to HSIN-JFOnet in order to optimize the sharing of situational awareness related to resource requirements.

2.6 Coordination Plans and Briefings

- Briefings and Coordination Plans will be posted by the HSOC representative to the Situation Unit.

3.0 External Communications

- The aggressive use of JFOnet to distribute information, including scheduled SITREPS and SPOTREPS, permits authorized external users and organizations, such as the HSOC, IIMG, State/local emergency management agencies, DHS components, and other appropriate Federal/State/local agencies, to engage in passive situational awareness monitoring or active collaboration as needed with the JFO.
- Agencies providing representatives to the JFO may elect to use intra-agency communications systems to exchange information with their JFO representative. Under such circumstances the agency's JFO representative will be responsible, to the extent permissible by agency policy and security practices, to post that information on JFOnet.

- The JFO's Logistics Section, Communications Unit, in tandem with HSOC personnel assigned to the JFO, shall coordinate communicating to all appropriate parties and organizations the instructions for accessing JFOnet.
- RFIs posed to the JFO from DHS headquarters' organizations or appropriate other agencies, to the greatest extent possible, shall be processed in accordance with the direction in 2.2 and 2.3 above.

4.0 Threat Monitoring and Initial Incident Assessment

The JFO's daily threat monitoring mission is to identify threats inside, at, or approaching the borders of the United States and pass that information to the HSOC as well as pertinent local Federal, State, and Local intelligence and law enforcement agencies. This process continues regardless of other incidents being addressed by the JFO Coordination Group. JFO incident assessment focuses on evaluating information received and making notifications and reports based on that evaluation. Additional emphasis is applied in trying to determine subsequent threats and whether the incident is terrorist related.

The JFO also provides situational awareness and facilitates coordination of local DHS assets and Incidents of National Significance as defined by the NRP.

HSPD-5 designates the HSOC as the "primary national-level hub for operational communications and information pertaining to domestic incident management." Timely incident reporting is required to enable the HSOC to accomplish its situational awareness mission for the national leadership (White House) and the Secretary of Homeland Security. It is critical that reports of possible terrorist activity or reports of potential significant disasters reach the HSOC as quickly as possible through the JFO from Federal, State, local, and tribal authorities as well as the private sector and NGOs. Only by rapidly sharing this information with the HSOC will DHS be ready to effectively coordinate any Federal response required or requested. In most cases, this occurs naturally through routine communications paths through department and agency operations centers.

5.0 Daily Production

On a daily basis, a number of products are generated by the JFO, each with its own production schedule, development team, and distribution.

5.1 JFO Input to the Secretary's Morning Brief (SMB)

The Secretary's Morning Brief is provided to the Secretary daily and is intended to provide the Secretary with his first briefing of the day. The report identifies the key incidents of the previous 24 hours, focusing on events of major significance, items that may solicit media attention, and items of unique interest to DHS. The production of this report is overseen by the Secretary's Briefing Team, but it is the responsibility of the HSOC Senior Watch Officer and Senior Intelligence Analyst to ensure that all items that should be brought to the Secretary's attention have been passed to the production team, that the content of the report is accurate, and that the report is provided on time to meet

the Secretary's schedule. A copy of the SMB is distributed to the White House Homeland Security Council Staff and to the Director of Central Intelligence. The SMB contains information at the highest levels of classification.

5.2 JFO Input to the Homeland Security Operations Morning Brief (HSOMB)

The HSOMB is prepared for the Secretary of Homeland Security and summarizes reports of suspicious activities received from DHS components, Federal, State, and local law enforcement agencies, and the private sector, during the previous 24 hours. The information provided has not been vetted or analyzed. Material in the HSOMB consists of data that have been subjected to that day's review process to determine whether any of these activities poses a threat to the United States. Those activities that are suspicious or may pose a potential threat are passed to the Office of Intelligence and Analysis (IA) and appropriate intelligence and law enforcement agencies for further analysis and action.

5.3 Reporting

Reports fall into three basic categories: Situation Reports (SITREPs), Homeland Security Intelligence Reports (HSIR), and Spot Reports (SPOTREPs). SITREPs can be used in any type of reporting format and usually list pertinent information covering specific periods of time. Intelligence reports are usually in two formats: those without access restrictions, HSIR, and ones with restricted access, HSIR-R. SPOTREPs are reports issued as incidents of such significance occur that immediate notification to the HSOC is warranted. Information in SPOTREPs is incorporated into SITREPs for the relevant time period. Reporting formats are included in Annex D.

6.0 Secure Video Teleconferences (SVTCs)

Twice daily (and on an as-needed basis dictated by a particular situation), a Secure Video Teleconference is held with the White House, members of the Intelligence Community, and key Federal law enforcement and response agencies. The purpose of the SVTC is to share information with the entire community and afford the opportunity for real-time reaction and response. SVTCs are normally held at 0900 and 1500 Monday through Friday. The morning conference is restricted to a limited number of agencies, and will normally include the PFO. The HSOC has a seat in the DHS SVTC group. In addition to the sharing of information, this session is designed to focus on cooperative efforts between the participating organizations. A weekend SVTC is frequently held at 1000 on Saturday. The schedule for weekend sessions is established at the Friday 1500 session. Afternoon and Saturday morning sessions also focus on information sharing, but encompass a larger viewing audience. The Senior Watch Officer is responsible for attending these meetings.

Information sharing on the part of DHS is typically focused on events at the borders, such as individuals with a questionable background interdicted at one of the ports of entry or border crossings, and on reports of suspicious activity. The PFO will report on new items, or provide supplemental information about an ongoing event at the JFO.

7.0 Situation Unit Watch Rotations

Watch rotations at the JFO Situation Unit are normally 12 hours in duration: 0700-1900 and 1900-0700. The relieving watch is expected to report for duty 30 minutes before their watch is scheduled to begin to allow for a proper turnover. When the relieving watch has not stood watch for a number of days, to establish situational awareness, they normally report to the JFO in excess of 30 minutes before their watch.

Whenever possible, integrity of watch teams is maintained throughout the cycle. This maximizes the cohesive bond between team members and optimizes team response in critical situations.

8.0 Logs

The JFO Watch Log is an official document. While it is the ultimate responsibility of the PFO, maintenance of the log may be delegated to personnel on watch. The log, equivalent to an ICS Unit Log, is intended to be a thorough documentation of the events that occurred during a particular watch, and identifies the JFO Coordination Group personnel present during the period covered. Logs are reviewed on a daily basis by all members of the JFO Coordination Group.

As an official record, under no circumstances are log entries changed after the log for a particular shift is closed out or there has been a turnover of watch personnel. If updated or corrected information becomes available, a new log entry is made, referencing the initial entry and providing the updated/corrected information. When this is done, adding a post-watch note at the place where the initial information was provided is acceptable, with the note directing the reader to the place in the log where the updated/corrected information may be found.

Watch relief is not effected until all log entries from the watch being relieved are completed. While it is the responsibility of the off-going watch to complete their logs, the incoming SWO does not accept turnover until he/she has read and understood all entries, and acknowledges them to be complete.

The daily log is closed at 2400 local time. All outstanding actionable entries are carried over and annotated at the beginning of the new log entry.

Tab 1 to Annex E: JFO "Battle Rhythm" Timeline

JFO Battle Rhythm Timeline (for use after JFO activation)	
0:00	• Event Reported to JFO
+0:05	• State/Local Connectivity Established/Confirmed
+0:10	• Notification to JFO Coordination Group
+0:15	• JFO Coordination Group Members Notified/Recall Initiated (JFO)
+1:00	• Initial SITREP 1 to HSOC • Initial Brief to HSOC/IIMG/Secretary (PFO/JFO Coordination Group)
+1:45	• Initial Press Release Decision • All JFO Coordination Group members assembled at JFO • Initial In-Brief/Assignments to JFO Coordination Group (PFO/Watch)
+2:00	• Initial White House VTC/HSC Principals Meeting (PFO/Secretary/IIMG Director)
+3:00	• VTC Briefback to HSOC/IIMG (PFO/IIMG Director)
+4:00	• Initial IIMG COA Brief to Secretary (IIMG Director)
+7:00	• SITREP 2 to HSOC / White House Situation Room (JFO/HSOC/IIMG Chief) – NLT 6 Hours from Initial SITREP

- **SITREPs daily at 0600, 1200, 1800 to the HSOC and White House (PFO/JFO Coordination Group/HSOC/IIMG Director).**
- **The PFO, HSOC Director, and the IIMG Director will decide when this reporting sequence begins, after the initial SITREP has gone out.**
- **Within 48 hours of the incident, the HSOC Director and the IIMG Director may decide to reduce the reporting period to 0600 and 1800.**
- **Follow-on briefings to the Secretary as required.**

Tab 2 to Annex E: Initial Situation Report (SITREP)

Serves as information/intelligence in-brief to IIMG members upon activation, as well as initial written communication to the White House.

Homeland Security Domestic Incident Management
Initial SITREP

1. **SITREP Number**
2. **Date/Time**
3. **Incident Type** (CBRNE, Mass Migration, Natural Disaster, etc.)
4. **Location**
5. **Time of Incident**
6. **Weather Conditions**
7. **Threat/Causal factors**
8. **Initial On-Scene Status/Capabilities Assessment**
   - ☐ Casualties (# of dead; # of hospitalized)
   - ☐ Property Damage
   - ☐ Infrastructure Affected
   - ☐ Terrorism Nexus
   - ☐ General Population Status
   - ☐ Weather Effects
   - ☐ Extent of Contamination
   - ☐ On-Scene/En Route Capabilities
   - ☐ Requests for Additional Support
   - ☐ Possible Cascading Effects
   - ☐ WMD Effects
   - ☐ Indications of Follow-On Incidents
9. **Initial Response** (on-scene assets, emergency operations centers activated, local/regional response/recovery capability, etc.)
   - ☐ Local
   - ☐ State
   - ☐ Federal
10. **Federal/State/Local/International/Private Sector Contacts Made**
11. **COOP/COG Actions Anticipated**
12. **NCR Impact**
13. **International Impact**
14. **DHS Initial Actions/Intentions** (warning/bulletin issuance, press release issuance, IIMG activation, White House notification, etc.)
15. **Additional Comments/Considerations**

Tab 3 to Annex E: Situation Update Reports

Provided to DHS/Interagency senior leadership and the White House on a pre-determined basis.

Domestic Incident Management
DHS Situation Update Report

SITREP NO:
DATE/TIME:

1. **On-Scene Update**
   - **A.** Casualties
   - **B.** Extent of Damage
   - **C.** Projections of Cascading Events/HAZMAT Footprint
   - **D.** Causal Factors
2. **Threat Update**
   - **A.** General Situation
   - **B.** Terrorism Nexus
   - **C.** HSAS Level
   - **D.** Potential for Additional Attacks/Incidents
   - **E.** WMD Considerations
3. **Security Issues/Operational Activities**
   - **A.** Borders and Coastal Waters
   - **B.** Transportation
   - **C.** Law Enforcement
4. **Critical Infrastructure Issues/Operational Activities**
   - **A.** Sector Impacts
   - **B.** Cross-Sector Impacts
   - **C.** Protective Measures/Sustainability
5. **Emergency Response Issues/Operational Activities**
   - **A.** Transportation
   - **B.** Communications
   - **C.** Public Works and Engineering
   - **D.** Firefighting
   - **E.** Information and Planning
   - **F.** Mass Care
   - **G.** Resource Support
   - **H.** Health and Medical Services
   - **I.** Urban Search and Rescue
   - **J.** Hazardous Materials
   - **K.** Food and Water
   - **L.** Energy
6. **Local/State Assets Currently Involved** (Type/Number)

Domestic Incident Management
DHS Situation Update Report
(continued)

SITREP NO:
DATE/TIME:

7. Additional Local/State Assets Anticipated and ETA (Type/Number)
8. Federal Assets Currently Involved (Type/Number)
9. Additional Federal Assets Directed and ETA (Type/Number)
10. Future Federal Responses Anticipated
11. Non-Governmental Assets Currently Involved (Type/Number)
12. Requests for Assistance or Emergency/Presidential Declarations
13. Incident Communications, Public Affairs, & Preparedness Information
14. Local/State Government, International, and Private Sector Issues/Activities
15. Additional Remarks

Tab 4 to Annex E: Urgent Situation (Spot) Reports

FROM: (JFO, INCIDENT NAME)
TO: DHS/HSOC

INFO: OPERATIONAL CHAIN

C L A S S I F I C A T I O N L E V E L (UNCLAS, SBU, SSI, FOUO, C, S, TS, TS/SCI)
SUBJECT: **URGENT** JFO SPOT REPORT

1. **OCCURRENCE//**
   - **DATE OF URGENT OCCURRENCE**/(Date in MMDDYY Format)//
   - **TIME OF OCCURRENCE**/(Time in HHMM Format)//
   - **LOCATION/**(location in clearest possible short description)//
2. **TYPE OF OCCURRENCE/** (In short, plain language, what happened?)//
   - **RELATED TO JFO MISSIONS?**/(Yes or No—Is this directly related to the incident of national significance for which the JFO was established?)//
   - **NARRATIVE**/(Describe what happened.)//
3. **IMMEDIATE JFO ACTION**/(Action being taken immediately by the JFO – don't wait, follow up with a detailed SITREP later containing full details of plan of action.)//
4. **APPARENT TERRORISM NEXUS**// (Yes or No – does the occurrence appear to have a terrorism nexus?)
5. **THREATS AND CAUSAL FACORS//**(Short narrative text)
6. **SPOTREP CONTACT/NAME**/Name of best POC in the JFO regarding the urgent occurrence)/(Phone number of POC)/(E-mail address of mishap POC)//

###

Tab 5 to Annex E: Threat Situation Report

DHS PFO COMBINED SITUATION REPORT			
(FOUO)			SITREP No.
From:	Principal Federal Official (PFO)		
To:	Secretary DHS		
CC:	Director, Office of Operations Incident Management Division/Interagency Incident Management Group/Director, Homeland Security Operations Center		
Period Covered:		Period Ending:	
Location Covered:			

Current Threat Level:	
Current Situation:	▪
Significant Activities: (Last 7 Days)	▪
Expected Activities: (Next 48 – 72 hrs)	▪
CURRENT THREAT ASSESSMENT	▪
REGIONAL INTELLIGENCE SUMMARY	▪

PRIORITIES

Principal Federal Official (PFO)

▪

DHS PFO COMBINED SITUATION REPORT	
(FOUO)	SITREP No.
FEMA Regional Response Coordination Center (RRCC)/FCO (NRP operations focus)	
▪	
FBI On-Scene Commander: (Law Enforcement focus):	
▪	
PROTOCOL OFFICER	
	▪
PUBLIC AFFAIRS INFORMATION	
Media	▪
Upcoming	▪
DHS OPERATIONS	
Office of Intelligence & Analysis	▪
Preparedness Directorate	▪
HSOC	▪
Science & Technology	▪
FEMA	▪
MACC	▪
United States Coast Guard	▪
State & Local Desk	▪
Transportation Security Administration	▪
Immigration & Customs Enforcement	▪

DHS PFO COMBINED SITUATION REPORT	
(FOUO)	SITREP No.
Customs & Border Protection	▪
Office of Private Sector Liaison	▪
Department of Health and Human Services	▪

LOGISTICS
▪ N/A
STATUS OF SUPPORT FACILITIES
▪ N/A
ASSESSMENT/LIMITING FACTORS
▪ None

Tab 6 to Annex E: Casualty Reports

FROM: (JFO, INCIDENT NAME)
TO: DHS/OFFICE OF OPERATIONS IMD
VIA: DHS/HSOC

INFO: OPERATIONAL CHAIN

C L A S S I F I C A T I O N L E V E L (UNCLAS, SBU, SSI, FOUO, C, S, TS, TS/SCI)
SUBJECT: JFO CASUALTY (or MISHAP)
//
WHAT FOLLOWS MAY CONTAIN PRIVILEGED SAFETY INFORMATION.
USE FOR MISHAP PREVENTION PURPOSES ONLY.
//

1. GENERAL INFO//

- **DATE OF INCIDENT**/(Date in MMDDYY Format)//
- **TIME OF INCIDENT**/(Time in HHMM Format)//
- **RELATED TO JFO MISSIONS?**/(Yes or No—Is this an operational mishap?)//
- **NARRATIVE**/(Describe the event – who, what, where, how)//
- **PRIMARY CAUSE**/(Primary cause of the casualty or mishap)//
- **CONTRIBUTING FACTORS**/(Additional factors contributing to the cause or severity of the incident)// (NA if none)
- **JFO ACTION**/(Action taken at the JFO to prevent this mishap from occurring again, if any is possible)//

2. PERSONAL INJURY DATA (subparagraphs for each injured person)//

- **DEATH?/** (Yes or No)
- **IS DEATH IMMINENT?**/ (Yes or No)
- **NOK NOTIFIED?** (Yes or No – have next of kin been notified?)
- **RANK OR GRADE**/(GS-12, for example)//
- **MILITARY RATE**/(MK, for example)//
- **STATUS**/(Status of the person at time of the incident; ON DUTY, OFF DUTY IN HOTEL, for example)//
- **PRIMARY INJURY**/(Primary body part injured)/(Nature of primary injury)//
- **SECONDARY INJURIES**/(Secondary body parts injured)/(Nature of secondary injuries)//
- **SEVERITY**/(LOST WORK, for example)//
- **PERSONAL PROTECTIVE USED**/(Type(s) of PPE used if this is an operational accident/injury)// (Each type separated by a "/")
- **PPE REQUIRED**/(Type(s) of PPE required by JFO supervisors for the operation)// (Each type separated by a "/")
- **DAYS HOSPITALIZED**/(Number of days hospitalized)//
- **DAYS LOST**/(Number of days of lost work time beyond the day of injury)//
- **DAYS REST**//(Number of days in a restricted or fit for light duty status)//

3. MISHAP PROPERTY DAMAGE (If any)//

- **JFO PROPERTY DESCRIPTION**/(Description of property damaged)//
- **JFO PROPERTY SOURCE**/(Agency, company, or other owner of the property)//
- **LOST OPERATIONAL DAYS**/(Number of operational days lost for the property or asset due to the mishap)//
- **ESTIMATED JFO PROPERTY VALUE AND REPAIR COSTS/$(**Rough estimate of value of property or cost to repair in $, 0.00 if none)
- **NON-JFO PROPERTY DAMAGE**/(Description of non-JFO property damaged during the mishap/accident, scope of damage, rough estimates of value and repair costs)//

4. INVESTIGATOR/NAME/(Name of mishap investigator)/(Phone number of mishap investigator)/(E-mail address of mishap investigator)//

###

Tab 7 to Annex E: HSIN-JFOnet Technical Data

[RESERVED]

Tab 8 to Annex E: Template JFO Information-Sharing Plan

Critical Information Requirement	Possible Essential Elements of Information	Proposed Methodology/Sources	Responsible Elements	Deliverable	Collection Suspense	On Arrival Distribute To
Boundaries of Disaster Area	Geographic locations sustaining damage Description of extent of damage sustained Boundaries of areas evacuated Estimated % of population evacuated Estimated % of population unable to return	Predictive modeling Geographic Information System (GIS) HAZUS, CATS, USGS Remote Sensing/Aerial Reconnaissance (NIMA) Assessment Teams Community Relations & ARC Reports State Liaison/ERT-A/FCO Reports News Media and other open sources State EM Office	JFO Planning Section	Summary of Impacts Map Situation Report Situation Briefing Daily Intelligence Summary	Modeling data as soon as available. Initial estimate NLT 12 hours following event Updated as new information becomes available or at least daily.	HSOC FEMA Ops Center ERT-A Leadership Assessment Teams PFO/FCO SCO JFO/JOC JFO/MACC
Access Points to Disaster Area	Traffic control points Best routes to reach local EOCs, Mobilization Points, Command Posts and other critical locations. Best airports for arriving staff to use Special permits or identification required to access disaster area.	State Emergency Management Office State Liaisons State Highway Department Reports State Patrol and Law Enforcement Reports Transportation Reports Operations	JFO Operations Section/Response & Recovery Branch/ESF #1	GIS Products Situation Briefing Situation Reporting Special Briefings	NLT 8 hours post event. Updated at least daily.	HSOC FEMA Ops Center ERT-A Leadership Assessment Teams PFO/FCO SCO JFO/JOC JFO/MACC
Jurisdictional Boundaries	List of jurisdictions (cities, counties) affected, with maps Political and congressional jurisdictions affected	State Liaison/ERT-A/FCO Reports News Media/Open Sources GIS Assessment teams Community Relations Reports Remote Sensing/Aerial Reconnaissance	JFO Planning Section/Situation Unit	GIS map with political jurisdiction boundaries GIS map with congressional districts Jurisdictional profiles	NLT 12 hours following event	HSOC FEMA Ops Center Assessment Teams PFO/FCO SCO & FCOs JFO/JOC JFO/MACC External Affairs

Critical Information Requirement	Possible Essential Elements of Information	Proposed Methodology/Sources	Responsible Elements	Deliverable	Collection Suspense	On Arrival Distribute To
Socio-economic/ Political Impacts	Number of homes affected Potential/estimated population affected Number of shelters open/population Potential shelter requirements	Predictive modeling Geographic Information System (GIS) Remote Sensing/Aerial Reconnaissance Assessment Teams Community Relations Reports State Liaison/ERT-A/FCO Reports	JFO Planning Section/XXX Unit	Situation Report Status Briefing Summary of Impacts Maps Daily Intelligence Summary Jurisdictional Profile	Initial estimate NLT 12 hours following event Updated as new information becomes available or at least daily.	HSOC FEMA Ops Center Assessment Teams PFO/FCO SCO & FCOs JFO/JOC JFO/MACC External Affairs
Socio-economic/ Political Impacts	Number and type of businesses affected	Predictive modeling GIS Remote Sensing/Aerial Reconnaissance Assessment Teams News Medial and other open sources	JFO Operations Section	Situation Report Inputs SBA Reports and Text Items Summary of Impacts Maps	Initial estimate NLT 12 hours following event Updated as new information becomes available or at least daily.	HSOC FEMA Ops Center Assessment Teams PFO/FCO SCO & FCOs JFO/JOC JFO/MACC External Affairs
Socio-economic/ Political Impacts	Congressional Districts Impacted	GIS Database Congressional Liaison Officer	JFO Planning Section/XXX Unit	Congressional Boundaries Map overlaid with disaster boundaries	NLT 12 hours following event	HSOC FEMA Ops Center Assessment Teams PFO/FCO SCO & FCOs JFO/JOC JFO/MACC Congressional Liaison Officer

Critical Information Requirement	Possible Essential Elements of Information	Proposed Methodology/Sources	Responsible Elements	Deliverable	Collection Suspense	On Arrival Distribute To
Hazard Specific Information	What are the characteristics of the disaster What are the special hazards associated with the event What are the short and long term impacts of the event Is this a short term or long term event	NOAA Reports USGS Reports Other sources as appropriate	JFO Planning Section	Situation Briefings Situation Reports Special reports and presentations	NLT 4 hour after event. Updated as needed	HSOC FEMA Ops Center Assessment Teams PFO/FCO SCO & FCOs JFO/JOC JFO/MACC
Seismic and/or Other Geophysical Information	Are there any ongoing seismic hazards Are there any geophysical conditions or elements that impact the disaster or event	USGS Reports COE Reports Remote Sensing Information	JFO Planning Section	Situation Briefings Situation Reports Special reports and presentations	NLT 4 hour after event. Updated as needed	HSOC FEMA Ops Center Assessment Teams PFO/FCO SCO & FCOs JFO/JOC JFO/MACC
Weather Conditions/ Forecasts	Are there any weather impacts occurring or forecast for the disaster or emergency area	NWS reports	JFO Planning Section	Situation Briefings Daily Intelligence Summary	Per forecast schedule appropriate to event.	HSOC FEMA Ops Center Assessment Teams PFO/FCO SCO & FCOs JFO/JOC JFO/MACC
Historical and Demographic Information	Has a similar event occurred in the past and what were the outcomes, response problems and impacts	Mitigation Reports NWS Reports NEMIS	JFO Planning Section	Special reports	NLT 12 hours following event	HSOC FEMA Ops Center Assessment Teams PFO/FCO SCO & FCOs JFO/JOC JFO/MACC

Critical Information Requirement	Possible Essential Elements of Information	Proposed Methodology/Sources	Responsible Elements	Deliverable	Collection Suspense	On Arrival Distribute To
Historical and Demographic Information	What are the demographics of the area What is the unemployment rate of the area	Mitigation Reports NWS Reports NEMIS	JFO Planning Section	Jurisdictional Profile Regional Write Ups	NLT 24 hours following event	HSOC FEMA Ops Center Assessment Teams PFO/FCO SCO & FCOs JFO/JOC JFO/MACC
Predictive Modeling Impact Projections	Who is coordinating predictive modeling What data inputs are being used What programs are being used What are the program biases Where are predictive modeling outputs available	State Local Government MAC EPA DTRA	JFO Planning Section/ NOAA	GIS Products and outputs showing areas of impacts, concentrations, and damage zones.	NLT 3 hours following event or sooner if possible	HSOC FEMA Ops Center Assessment Teams PFO/FCO SCO & FCOs JFO/JOC JFO/MACC
Initial Needs and Damage Assessments	Have there been PDA requests What is the status of the PDA What is the status of the RNA What are the findings of the PDA What are the findings of the RNA	State Liaison State Emergency Management PDA Teams RNA Teams NEMIS	JFO Operations Section	Impacts Map Situation Report Jurisdictional Profile Daily Intelligence Summary	NLT 3 hours post request or gathering of information	HSOC FEMA Ops Center Assessment Teams PFO/FCO SCO & FCOs JFO/JOC JFO/MACC

Critical Information Requirement	Possible Essential Elements of Information	Proposed Methodology/Sources	Responsible Elements	Deliverable	Collection Suspense	On Arrival Distribute To
Status of Communications Systems	Status of telecommunications service (including Internet) and infrastructure, including towers Reliability of cellular service in areas affected Potential requirement for radio/satellite communications capability Status of emergency broadcast (TV, radio, cable) system and ability to disseminate information	State Liaison/ERT-A/FCO ESF #2 News Media/open sources Telephone companies NCS member agencies	JFO Operations Section/ Response & Recovery Branch/ESF #2	Input for situation report and/or verbal report NCS Situation Report	Initial estimate NLT 12 hours following event Updated as new information becomes available or at least daily.	HSOC FEMA Ops Center Assessment Teams PFO/FCO SCO & FCOs JFO/JOC JFO/MACC External Affairs VolAg
Status of Transportation	Status of all modal systems, air, sea, land, rail Status of major/primary roads Status of critical and non-critical bridges Status of transcontinental/regional natural gas and fuel pipelines Status of evacuation routes Status of public transit systems Accessibility concerns Debris issues	State Liaison/ERT-A/FCO Reports State Department of Transportation ESF #1 Assessment team reports Community Relations U.S. Army Corps of Engineers USCG Captain of the Port Remote sensing/aerial reconnaissance Predictive modeling	JFO Operations Section/Response & Recovery Branch/ESF #1	Input for situation report and/or verbal report DOT Situation Report GIS products	Initial estimate NLT 12 hours following event Updated as new information becomes available or at least daily.	HSOC FEMA Ops Center Assessment Teams PFO/FCO SCO & FCOs JFO/JOC JFO/MACC External Affairs

Critical Information Requirement	Possible Essential Elements of Information	Proposed Methodology/Sources	Responsible Elements	Deliverable	Collection Suspense	On Arrival Distribute To
Status of Emergency Operations Centers	Status of local EOCs Status of State EOC Status of Agency EOCs Location and status of Federal facilities established	State Liaison/ERT-A/FCO ESFs/Other Federal Agencies Regional Offices RST	JFO Operations Section	Operations Section input to situation report and/or verbal report GIS products	Initial estimate NLT 12 hours following event Updated as new information becomes available or at least daily.	HSOC FEMA Ops Center Assessment Teams PFO/FCO SCO & FCOs JFO/JOC JFO/MACC
Status of critical infrastructure and facilities	Status of Acute Medical Care Facilities Status of Chronic Medical Care Facilities Status of Home Health Agencies Status of State and Local Health Departments Status of State/Local EMS Systems Status of VA Medical Systems	Reports from ESF #8 Reports from Community Relations State Reports	JFO Operations Section	ESF 8 input to the situation report and/or verbal reports PHS Situation Reports GIS products	Initial estimate NLT 12 hours following event Updated as new information becomes available or at least daily.	HSOC FEMA Ops Center Assessment Teams PFO/FCO SCO & FCOs JFO/JOC JFO/MACC
Status of critical infrastructure and facilities	Status of public water supply systems Status of private water supply systems Status of public wastewater systems Status of private septic systems	ESF #8 Reports ESF #3 Reports State & Local Health Department Reports State	JFO Operations Section / JFO Infrastructure Liaison	ESF#3, 8 and 12 inputs to the situation report and/or verbal reports USACE, PHS and DOE Situation Reports GIS products	Initial estimate NLT 12 hours following event Updated as new information becomes available or at least daily.	HSOC FEMA Ops Center Assessment Teams PFO/FCO SCO & FCOs JFO/JOC JFO/MACC

Critical Information Requirement	Possible Essential Elements of Information	Proposed Methodology/Sources	Responsible Elements	Deliverable	Collection Suspense	On Arrival Distribute To
Status of Energy Systems	Status of electrical power generation and distribution facilities	Reports from ESF #3 & ESF #12 State Reports Media Open Sources	Primary Operations Supporting State	ESF 3 and 12 inputs to the situation report and/or verbal reports GIS products	Initial estimate NLT 12 hours following event Updated as new information becomes available or at least daily.	HSOC FEMA Ops Center Assessment Teams PFO/FCO SCO & FCOs JFO/JOC JFO/MACC
Resource shortfalls	What are the actual or potential resource shortfalls of the affected State What are the anticipated requirements for Federal resources What are potential or actual Federal shortfalls What are potential sources for resource shortfalls What resources are available and where are they located Priorities: water, food, power, medical, heat, communications	State Liaison State Coordinating Officer RST EST Logistics Reports Assessment Team reports Community Relations field reports ESF reports	JFO Logistics Section	Territorial Resource Center Inventories Time-Phased Deployment Lists Status Briefing Agency/ESF Reports Daily Intelligence Summary	Initial estimate NLT 12 hours following event Updated as new information becomes available or at least daily.	HSOC FEMA Ops Center Assessment Teams PFO/FCO SCO & FCOs JFO/JOC JFO/MACC

Critical Information Requirement	Possible Essential Elements of Information	Proposed Methodology/Sources	Responsible Elements	Deliverable	Collection Suspense	On Arrival Distribute To
Status of declarations	Has the Governor Requested Assistance and for what and where Is the Governors request a normal or expedited one Who is completing the Regional Disaster Summary and Analysis and Recommendation Is there a Presidential Declaration and if so what type Which jurisdictions are included Which types of assistance are authorized Are there special cost-share provisions for Direct Federal Assistance	Governor's Request Letter Regional Disaster Summary Regional Analysis and Recommendation NEMIS Entries Notice of Disaster Declaration	JFO Operations Section	Disaster Fact Sheet GIS products showing declared counties and type of assistance	Within 1 hour following official announcement .	HSOC FEMA Ops Center Assessment Teams PFO/FCO SCO & FCOs JFO/JOC JFO/MACC
Status of ESF Activations	Which ESFs are activated in the JFO? Are sufficient numbers of ESF representative available to staff required JFO sections?	Mission Assignment Logs Operations Section	JFO Operations Section	Ops input to situation report and/or verbal report Mission Assignment lists	Within 3 hours of activation	HSOC FEMA Ops Center Assessment Teams PFO/FCO SCO & FCOs JFO/JOC JFO/MACC
Major issues/ activities/ Mission Assignments of ESFs/OFAs	What operations and assessments are agencies conducting under their own authorities What mission assignments have been issued What is status of Mission Assignments	Mission Assignment logs ESF/Agency situation reports Functional plans RRCC/ERT-A	JFO Operations Section	Situation Report, displays, Action Plan	Initial estimate NLT 12 hours following event Updated as new information becomes available or at least daily.	HSOC FEMA Ops Center Assessment Teams PFO/FCO SCO & FCOs JFO/JOC JFO/MACC

Critical Information Requirement	Possible Essential Elements of Information	Proposed Methodology/Sources	Responsible Elements	Deliverable	Collection Suspense	On Arrival Distribute To
Status of key personnel	Who and where is: ERT-A Team Leader PFO/FCO SCO & FCOs RRCC Director FEMA liaison to State JFO Section Chiefs Key Support Staff	Regional Response Coordination Center Initial Operating Reports State Liaison/ERT-A/FCO	JFO Operations Section	Initial Operating Report Disaster Fact Sheet	Upon Activation of the FRP Within 4 hours following Disaster Declaration	HSOC FEMA Ops Center Assessment Teams PFO/FCO SCO & FCOs JFO/JOC JFO/MACC
Status of remote sensing operations	What Remote Sensing Mission have ESF's undertaken under their own authority What remote sensing missions have the State and Local governments undertaken under their own authority What remote sensing missions have been already tasked by RST, ERT & EST What are the available assets to provide remote sensing data What format and when will information be available Who is providing interpretation of incoming data How will data be shared	Operations Section and ESF Reports State Liaison and State Reports CAP Reports Mission Assignment Logs	JFO Planning Section	Remote Sensing imagery derived products Text interpretive reports	On-going	HSOC FEMA Ops Center Assessment Teams PFO/FCO SCO & FCOs JFO/JOC JFO/MACC

Critical Information Requirement	Possible Essential Elements of Information	Proposed Methodology/Sources	Responsible Elements	Deliverable	Collection Suspense	On Arrival Distribute To
Priorities for Response	What are the Federal operational priorities	RRCC Director Principal Federal Official Federal Coordinating Officer JFO Coordination Group	JFO Planning Section	JFO Coordination Plan Situation Report Status Briefing	As established Every C-Period	HSOC FEMA Ops Center PFO/FCO SCO & FCOs JFO sections
Recovery Program Statistics	What are the statistics for IA, PA, and HM What are the trends they show What do the figures mean in real terms	NEMIS Reports Analysis Reports	JFO Operations Section	Situation Briefing Situation Report	At beginning of every C-Period for previous reporting period	PFO/FCO SCO & FCOs JFO sections
Donations/ Voluntary Agency Activities	Has a Donations Hotline been established or is there a need for the Hotline Which Voluntary Agencies are actively involved in operations	VOLAG Reports Voluntary Agencies Agency/ESF reports	JFO Operations Section	Situation Report Status Briefing	Updated as new information becomes available or at least daily.	HSOC FEMA Ops Center PFO/FCO SCO & FCOs JFO sections
Upcoming activities	What is the schedule of daily meetings and briefings What other significant events of activities are planned or scheduled	Federal Coordinating Officer ERT-A Team Leader RRCC Director State Coordinating Officer Planning Support Branch Chief	JFO Planning Section	Daily Meeting Schedule	On-going (Publish every O-Period)	HSOC FEMA Ops Center RRCC PFO/FCO SCO & FCOs
Status of Efforts Under Other Federal Emergency Plans and Authorities	What are other agencies doing under their own authority	Operations	JFO Operations Section	Situation Reports Situation Briefings	Initial report NLT 12 after event. Updated daily.	HSOC FEMA Ops Center PFO/FCO SCO & FCOs JFO sections

Critical Information Requirement	Possible Essential Elements of Information	Proposed Methodology/Sources	Responsible Elements	Deliverable	Collection Suspense	On Arrival Distribute To
Safety Hazards	Is there a need for personnel protection equipment What are the safety hazards in conducting operations	Community Relations Field Reports Assessment Team reports State Liaison/ERT-A/FCO Predictive Modeling	Primary Safety Support JFO Operations Section JFO Security Officer	Safety Briefings Safety Messages	Initial estimate NLT 12 hours following event Updated as new information becomes available or at least daily.	HSOC FEMA Ops Center PFO/FCO SCO & FCOs JFO sections Assessment Teams External Affairs
Hazardous, toxic and radiological issues	Are there reported or suspected hazardous material/toxic release incidents What follow up actions are planned or underway Are there actual or potential radiological incidents What follow up actions are planned or underway	State Liaison/ERT-A/FCO ESF #10 Lead Federal Agency (LFA) under the Federal Radiological Response Plan (FRERP) Nuclear Regulatory Commission (NRC) Remote Sensing Predictive modeling GIS Databases	Primary Operations Support JFO Planning Section	Status Briefings Situation Reports GIS products	Initial estimate NLT 12 hours following event Updated as new information becomes available or at least daily.	HSOC FEMA Ops Center JOC PFO/FCO SCO & FCOs JFO sections Assessment Teams JFO Safety Coordinator JFO Security Officer

Annex F: Security Procedures

Tab 1 to Annex F: SOP for Information Classification and Handling

1.0 Purpose

This Standard Operating Procedure (SOP) provides guidance on the security measures that will be implemented and adhered to for the handling, storage, transmission, reproduction, and destruction of Classified National Security Information (NSI).

2.0 Applicability

This SOP applies to all personnel working in or around the Joint Field Office (JFO). It is the responsibility of the JFO Security Officer to enforce these procedures through the JFO Physical and Information Security Plan. All persons authorized unescorted access to the JFO will read and be familiar with the requirements of this SOP.

3.0 Access

Access to classified information shall be limited to persons whose official duties require knowledge or possession of the information. No one has a right to have access to classified information solely by virtue of office, rank, or position**.** Three criteria shall be met prior to granting access:

3.1. Security Clearance

The intended recipient has been granted a security clearance equal to or higher than the level of classified information to which access will be granted.

3.2. Need-to-know

The intended recipient has a need-to-know the information in the performance of official governmental duties. The responsibility for determining whether an individual possesses the need-to-know for access to classified information rests with the authorized holder of the information. Where the authorized holder of the information is uncertain as to an intended recipient's need-to-know, he/she should contact the JFO Security Officer or the originator of the classified information.

3.3.

Where access involves the physical transfer of classified materials from one cleared person to another, the intended recipient has the means to properly store the materials.

4.0 Storage

Classified information shall be secured under conditions adequate to prevent access by unauthorized persons. The requirements specified in this SOP represent acceptable security standards. Security requirements for Sensitive Compartmented Information Facilities (SCIFs) are established by the Director of Central Intelligence through various Director of Central Intelligence Directives (DCIDs), and can be found in a separate SOP.

4.1.
Classified information that is not under the personal control and observation of an authorized person is to be guarded or stored in a locked security container, vault, room, or area, as follows:

4.1.1. Top Secret
Top Secret information shall be stored in a GSA-approved security container. One or more of the following supplemental controls must also be in place:

4.1.1.1. The location that houses the security container is subject to continuous protection by cleared guard or duty personnel;

4.1.1.2. Cleared guard or duty personnel inspect the security container once every 2 hours;

4.1.1.3. An Intrusion Detection System (IDS) is in place with personnel responding to the alarm arriving within 15 minutes of the alarm annunciation;

4.1.1.4. Security-In-Depth, as determined by the JFO Security Officer, when the GSA-approved container is equipped with a lock meeting Federal Specification FF-L-2740; or

4.1.1.5. Modular vault, vault, or a secure room constructed in accordance with guidance issued by DHS Office of Security and equipped with an IDS, with the personnel responding to the alarm within 15 minutes of the alarm annunciation if the area is covered by Security-In-Depth, or a 5-minute alarm response time if it is not. (Other rooms that were approved for the storage of Top Secret in the United States may continue to be used.)

4.1.2. Secret
Secret information shall be stored by one of the following methods:

4.1.2.1. In the same manner as prescribed for TOP SECRET information;

4.1.2.2. In a GSA-approved security container or vault without supplemental controls;

4.1.2.3. In a secure room that is approved for the open storage of SECRET information;

4.1.2.4. Until October 1, 2012, in a non-GSA-approved container having a built-in combination lock or in a non-GSA-approved container secured with a rigid metal lock bar and a GSA-approved padlock. When stored in a non-GSA-approved container, one or more of the following supplemental controls must be in place:

- The location that houses the container is subject to continuous protection by cleared guard or duty personnel;

- Cleared guard or duty personnel shall inspect the security container once every 4 hours; or

- An IDS with the personnel responding to the alarm arriving within 30 minutes of the alarm.

4.1.3. Confidential

CONFIDENTIAL information shall be stored in the same manner as prescribed for TOP SECRET or SECRET information except that supplemental controls are not required.

4.1.4.

GSA-approved field safes and special purpose one- and two-drawer, light-weight security containers, approved by the GSA, are used primarily for storage of classified information in the field. Such containers shall be securely fastened to a permanent structure or under sufficient surveillance to prevent their theft.

4.1.5. Combinations to Containers and Vaults

4.1.5.1. Only persons having an appropriate security clearance and need-to-know shall change combinations to security containers, vaults, and secure rooms used for the storage of classified information.

4.1.5.2. The combination of a container, vault, or secure room used for the storage of classified information shall be treated as information having a classification equal to the highest category of the classified information stored therein. Any written record of the combination shall be marked with the appropriate classification level. Standard Form 700, Security Container Information, will be used for this purpose.

4.1.5.3. Combinations shall be changed:

- When placed in use;

- Whenever an individual knowing the combination no longer requires access to it, unless other sufficient controls exist to prevent access to the lock;

- When the combination has been subject to possible compromise; or

- When taken out of service. Built-in combination locks shall then be reset to the standard combination 50-25-50; combination padlocks shall be reset to the standard combination 10-20-30.

5.0 Open Storage

An Open Storage Area is established when the volume or bulk of classified materials, or the functions associated with the processing of classified information, make the use of security containers impractical. The area designated for open storage serves as the container for the storage of classified materials and security measures must be in place and maintained in order to ensure the integrity of the materials stored therein.

5.1.

The JFO Security Officer will be contacted prior to any modifications being made to the structure or security devices that were in place at the time open storage was approved.

5.2.

Under no circumstances will the level of classified materials *openly* stored in the area exceed the level of open storage authorized.

5.3.

A copy of the open storage approval memorandum and the Open Storage Survey Report will be maintained as attachments to this SOP.

5.4.

Identifying Data.

Program Office Responsible for Area	(Self-Explanatory)
Position/Title of Responsible Official	(Enter the position and/or title of the person designated as a point of contact for the designated area)
Room Number(s) of Designated Area	(Enter the specific room number(s) of the area designated for open storage)
Address	(Enter the full address of the facility that houses the open storage area)
Highest Level of OPEN Storage Authorized	(Circle One) CONFIDENTIAL SECRET TOP SECRET

5.5. Procedures

5.5.1. Security Controls

5.5.1.1. Key locks, cipher locks, and card readers are supplemental access control devices only and do not provide sufficient security for an unattended open storage area. Therefore, whenever the designated area is unattended, all locking devices (built-in dial-type combination lock, key/cipher lock, electric strike, electric knob,

magnetic lock) will be in the locked position. The dial on the combination lock will be spun at least four times to ensure the combination is cleared. **The area will never be left open or unlocked when not occupied by an authorized person.**

5.5.1.2. The combination of the built-in dial-type combination lock is classified at the same level as the highest classification of materials stored therein. It will not be provided to any person that does not have the appropriate security clearance and need-to-know. The combination will be recorded on a Standard Form 700, Security Container Information, and appropriately stored by the JFO Security Officer.

5.5.1.3. At a minimum, the combination to the built-in dial-type combination lock will be changed every 2 years or immediately when the lock is first placed in service, when someone having knowledge of the combination terminates employment or is reassigned, if it is suspected that the combination was compromised, or if the area is found unattended and unlocked. Contact the JFO Security Officer for information on changing combinations.

5.5.1.4. The combination to a cipher lock and/or keys to a key lock will be handled as sensitive information/materials and provided only to persons with a need-to-know.

5.5.1.5. The combination to a cipher lock or the key lock will be changed/rekeyed as determined by the JFO Security Officer or responsible official.

5.5.1.6. When a card reader is used for supplemental access control, the reader will be programmed with its own distinct access level. Only persons who are authorized access to the area will have their key cards programmed to access the area.

5.5.1.7. Portable Electronic Devices (PEDs) shall not be introduced into an open storage area without written approval from the Designated Approval Authority in consultation with the cognizant Information Systems Security Manager and JFO Security Officer. Approvals will be considered only when the risks associated with the use of such equipment are clearly identified and sufficiently mitigated. Restrictions on the introduction of PEDs into open storage areas shall be prominently posted.

5.5.1.8. Intrusion Detection Systems (IDS). As IDS designs, specifications, and reporting procedures vary widely, the procedures for operation of an IDS will be prepared locally by the JFO Security Officer. Procedures should include as a minimum: Opening (disarming the IDS); Closing (arming the IDS); Alarm Response; IDS Maintenance; IDS Operations Checks; and procedures during a power outage.

5.5.2. Access Control

5.5.2.1. Only persons who have been granted a security clearance equal to or higher than the level of classified material stored in the facility, and who have a need-to-know, will be authorized unescorted access to the area.

5.5.2.2. Persons who do not have a security clearance equal to or higher than the level of classified material stored, and/or do not have a need-to-know, will not be allowed unescorted access to the area. Should the need arise to allow such visitors access to the area, the area will first be sanitized by a cleared person to ensure that no classified information is exposed or could otherwise be subjected to compromise. The visitor will then be escorted by a cleared person and will remain under visual escort for the duration of the visit.

5.5.2.3. When uncleared visitors are escorted into the area, the escort will announce to all persons working in the area that a visitor is present. In larger areas, if a strobe light is installed as a means for announcing visitors, it will be activated.

5.5.3. End-of-Day Security Checks

5.5.3.1. At the end of each duty day the area will be checked to ensure that it is secure. The Standard Form 701, Activity Security Checklist, will be used to record the end-of-day check.

5.5.3.2. The end-of-day check will be conducted by a cleared person designated by the JFO Security Officer.

5.5.3.3. The end-of-day check will consist of physically spinning the dial of the built-in combination lock at least four times in one direction. The supplemental access control device (i.e., key lock, cipher lock, card reader) will then be unlocked and the checker will physically tug on the door to make sure the dial-type combination lock is locked. The checker will also ensure that the IDS (if applicable) is armed.

5.5.3.4. Any discrepancies noted in the end-of-day check will be reported to the responsible official and/or the local security official.

5.5.4. Emergency Procedures

5.5.4.1. In the event an emergency arises that causes the immediate evacuation of the area, every reasonable effort will be made to properly secure the area prior to departure. However, personal safety will not be jeopardized in order to secure the area.

5.5.4.2. Should immediate evacuation prohibit the area from being properly secured, then upon termination of the emergency a reasonable effort will be made to verify that the integrity of the materials stored therein has not been compromised. This will include a visual inspection of the stored materials to determine if any items may be missing or tampered with. In addition, the combination to the built-in dial-type combination lock will be changed.

5.5.4.3. Any situation that is observed that affects the security integrity of the designated area, or the materials stored therein, will be reported immediately to the JFO Security Officer.

6.0 Transmittal

Classified information shall be transmitted and received in a manner that ensures tampering can be detected, inadvertent access is precluded, and timely delivery to the intended recipient is assured. Persons transmitting classified information are responsible for ensuring that intended recipients are authorized to receive the information, aware of the transmission, and have the capability to properly safeguard it. Under no circumstances will classified information be transmitted by any means other than the approved methods described in this SOP.

6.1. Methods of Transmission or Transportation

6.1.1.
TOP SECRET information shall be transmitted by:

6.1.1.1. Direct contact between appropriately cleared persons.

6.1.1.2. Secure telephone unit or equipment (STU III/STE) or Secure Fax keyed to the TOP SECRET level.

6.1.1.3. Defense Courier Service (DCS) or other authorized Government agency courier service.

6.1.1.4. Department of State Courier System (also known as a diplomatic pouch).

6.1.1.5. Electronic means over NSA-approved cryptographic communications system(s).

6.1.1.6. Under no circumstances will TOP SECRET information be transmitted via the U.S. Postal Service or any other uncleared commercial delivery service.

6.1.2.
SECRET and CONFIDENTIAL information shall be transmitted by any of the following means:

6.1.2.1. Any of the methods approved for transmitting TOP SECRET.

6.1.2.2. U.S. Postal Service Registered Mail.

6.1.2.3. U.S. Postal Service Express Mail. When using U.S. Postal Service Express Mail, the Waiver of Signature and Indemnity block (Item 11-B) on the U.S. Postal Service Express Mail Label shall not be executed. Additionally, street-side collection boxes shall not be used.

6.1.2.4. Commercial carriers or cleared commercial messenger services cleared for such purpose under the National Industrial Security Program Operating Manual (NISPOM).

6.2. Preparation of Material for Transmission

6.2.1. Envelopes or Containers

6.2.1.1. All classified information physically transmitted outside Government facilities shall be enclosed in two layers, both of which conceal the contents, prevent inadvertent opening, and would provide reasonable evidence of tampering. When envelopes are used, they shall be sealed with reinforced tape.

6.2.1.2. The inner enclosure shall clearly identify the name of the intended recipient, the address of both the sender and the recipient, the highest classification level of the contents, and any appropriate warning notices.

6.2.1.3. The outer enclosure shall clearly identify the office of the recipient and the address of both the sender and the recipient. There will be no markings on the outside envelope to indicate that the contents are classified. Intended recipients shall be identified by name only on the inner envelope. The following exceptions apply:

- If the classified information is an internal component of a packable item of equipment, the outside shell or body may be considered as the inner enclosure provided it does not reveal classified information;

- If the classified information is an inaccessible internal component of a bulky item of equipment, the outside or body of the item may be considered to be a sufficient enclosure provided observation of it does not reveal classified information;

- If the classified information is an item of equipment that is not reasonably packable and the shell or body is classified, it shall be concealed with an opaque enclosure that will hide all classified features;

6.2.1.4. Specialized shipping containers, including closed cargo transporters or diplomatic pouch, may be considered the outer enclosure when used; and

6.2.1.5. When classified information is hand-carried outside a facility, a locked briefcase or similar locking container may serve as the outer enclosure.

6.2.2. IT Equipment

The classified hardware, which will normally be laptop computers and/or removable hard drives, must be transported using a locking briefcase or similar lockable container. Any classified information transported in computer systems or media must be encrypted prior to transport.

6.2.2.1. Laptop Computer

- The computer and/or hard drive must be properly marked with an SF 706 - Top Secret label, SF 707 - Secret label, or SF 708 - Confidential label, as applicable.
- The computer must be turned off and all accessories needed for operation placed inside the laptop carrying case.
- Place the computer and all needed diskettes into the lockable container and lock.
- Place no classification markings on the exterior of the locking container. However, attach an address label that identifies an appropriate address to which the case should be shipped in the event it is separated from the courier.

6.2.2.2. Removable Hard Drive.

- The hard drive will be properly marked with an SF 706 - Top Secret label, SF 707 - Secret label, or SF 708 - Confidential label, as applicable.
- The hard drive and any needed diskettes will be inserted into a protective case that offers protection from visual inspection should the outer container be opened.
- The protective case containing the hard drive and applicable diskettes will be placed into a lockable container and locked.
- Place no classification markings on the exterior of the locking container. However, attach an address label that identifies an appropriate address to which the case should be shipped in the event it is separated from the courier.

6.2.2.3. Removable Media.

- Ensure they are marked using an SF 706 - Top Secret label, SF 707 - Secret label, or SF 708 - Confidential label, as applicable.
- Removable media will be packaged in accordance with paragraph 2 above.

6.3. Transport of Classified Material Within an Activity or Office

6.3.1.

If required to transport classified material from one building to another via a public street or road, courier authorization is required, and the material shall be packaged in accordance with the requirements of this SOP.

6.3.2.
If required to transport classified material within the same building or compound, an appropriate cover sheet shall be affixed to the document and the document shall be placed in an unmarked envelope or folder to avoid undue attention. Courier authorization is not required.

6.3.3.
Upon arrival at your destination, proceed directly to the approved facility to deliver or store the material. Ensure that appropriate storage is available at the point of destination (i.e., GSA-approved security containers for collateral classified materials; approved facilities for SCI). DO NOT leave classified packages in unattended offices.

6.3.4.
Ensure the recipient has an appropriate security clearance and a need-to-know. Do not leave classified material with any person other than the intended recipient unless you have verified that individual's security clearance and authority to act as the recipient's agent.

6.3.5.
It is also your responsibility to inform the intended recipient of the classification of the materials, and any additional security requirements.

6.3.6.
Ensure receipts are prepared and signed.

6.3.7.
The procedures provided below apply to the local transport of classified materials (from building to building within the local commuting area). When a need arises to transport classified materials aboard a commercial aircraft, prior approval must be obtained from the JFO Security Officer. Before approval is granted, the requester must provide sufficient justification as to why the materials must be hand-carried vice the use of other approved means, such as U.S. Postal Service Registered Mail for Secret and Confidential materials.

6.4. Transport of Classified Material by Courier

6.4.1.
The Courier Card or Courier Authorization Letter, along with Government identification, badge, or credentials, will be immediately available for presentation upon request by an appropriate security or law enforcement authority.

6.4.2.
When transporting classified materials within the local area, the courier will proceed directly to the destination with no unnecessary convenience stops.

6.4.3.
The materials being transported will remain in the courier's physical possession at all times while in transit. Classified material will not be left in hotel rooms, hotel safes, private residences, public lockers, unattended vehicles, etc.

6.4.4.
If overnight stops are anticipated, **arrangements must be made prior to departure** to store the materials at the nearest approved storage facility (military installation, U.S. Government Federal Facility, or cleared contract facility with approved storage authorization at the same level or higher than the materials you are carrying). In the event of unanticipated overnight stops, contact will be made with the nearest facility as identified above for proper storage.

6.4.5.
When in-transit storage is used at an approved facility, the package(s) will remain sealed and receipts will be used.

6.4.6.
Packages will never be opened, read, displayed, or otherwise viewed in any manner in public conveyances or places. This includes aircraft, restaurants, taxis, trains, etc.

6.4.7.
With the exception of paragraph 10 below, under no circumstances will a laptop computer containing classified information be placed in use while in transit.

6.4.8.
Packages will not be stored in any detachable storage compartments such as automobile trailers, luggage racks, vehicle trunks, passenger compartments, aircraft travel pods, or drop tanks.

6.4.9.
When traveling by commercial passenger aircraft within the U.S., classified material will be transported in your carry-on luggage. Prior authorization from the JFO Security Officer is required. Unless special circumstances exist, the hand-carried materials will be subjected to x-ray screening. If necessary, the screening official may also be allowed to feel, flex, and weigh the package without opening the envelopes themselves. The person screening the package will not, under any circumstances, be allowed to open the package. Should an attempt to open the package occur, request that the screening official have an airport security supervisor respond. If the situation cannot be remedied without the package being opened, contact the official cited on your courier authorization before proceeding.

6.4.10.
When requested by the screening official, a courier may "boot up" a laptop computer provided sufficient protection is provided to prevent against unauthorized disclosure of

classified information. IT equipment (laptop computers) must be configured to ensure that classified information does not become visible during the boot-up process.

6.4.11.
Travel directly from the office sending the material to the point of destination.

6.5. Record Keeping

An inventory of the classified materials being transported shall be recorded and maintained. The reason for this is so a record of the materials transported is available in the event something happens in transit, such as a package is lost.

7.0 Reproduction

Documents and other materials containing classified information shall be reproduced only when necessary to accomplish the mission of the JFO. The use of technology that prevents, discourages, or detects unauthorized reproduction of classified information is encouraged.

7.1. Approval for Reproduction

Unless restricted by the originating agency, TOP SECRET, SECRET, and CONFIDENTIAL information may be reproduced to the extent required by operational needs. For accountability purposes, reproduction of TOP SECRET information will be coordinated through the Top Secret Control Officer (TSCO).

7.1.1.
The following conditions must be met:

7.1.1.1. Classified material is not reproduced on equipment that poses unacceptable risks, for example, machines that are connected to an unclassified LAN, equipped with remote diagnostics, equipped with an internal memory, or in some other way retain images;

7.1.1.2. Reproduced material is clearly identified as classified at the applicable level;

7.1.1.3. Reproduced material is placed under the same accountability and control requirements as apply to the original material; and

7.1.1.4. Waste products generated during reproduction are properly protected and disposed of.

8.0 Accountability

8.1. Top Secret

8.1.1. Top Secret Control Officer (TSCO)

The JFO Security Officer will serve as the primary TSCO to manage the TOP SECRET Control Account (TSCA). Officials appointed as TSCO will possess a final Top Secret security clearance. The TSCO will maintain records for the accountability, dissemination, and destruction of TOP SECRET information. All TOP SECRET information will be processed (incoming and outgoing) to and through the TSCO.

8.1.1.1. Top Secret Document Register: A TOP SECRET Document Register will be maintained by the TSCO to record the receipt, disposition, and destruction of TOP SECRET information. DHS Form 11000-03, Document Control Register, Top Secret National Security Information, may be used for this purpose.

8.1.1.2. Top Secret Control Number: Each TOP SECRET document entered into the TSCA will be assigned a document control number (DCN). The DCN will consist of the office identifier, or other coding information, indicating the specific office possessing the document, the calendar year, and a sequential number indicating the number of documents generated/received within the calendar year.

8.1.1.3. Top Secret Signature Record: Each TOP SECRET document in the TSCA will have attached to it a TOP SECRET Signature Record, DHS Form 11000-04. Each person having access to the TOP SECRET information will sign and date the form indicating they had access.

8.1.2. Secret and Confidential

Except as required by the originator or as specified for certain categories of SECRET and CONFIDENTIAL information, there is no requirement to maintain accountability records or conduct inventories for SECRET and/or CONFIDENTIAL information.

9.0 Destruction

Classified documents and other materials shall be retained by the JFO only if they are required for effective and efficient operation of the organization, or if law or regulation requires their retention. Documents that are no longer required for operational purposes shall be disposed of in accordance with the provisions of the Federal Records Act and appropriate implementing directives and records schedules. Material that has been identified for destruction shall continue to be protected, as appropriate for its classification, until it is actually destroyed. Destruction of classified documents and materials shall be accomplished by means that eliminate risk of reconstruction of the classified information they contain.

9.1. Methods and Standards

9.1.1.

Classified information identified for destruction shall be destroyed completely to preclude recognition or reconstruction of the classified information. Methods and equipment used to routinely destroy classified information include burning, cross-cut shredding, wet-pulping, mutilation, chemical decomposition, or pulverizing.

9.1.2.
Cross-cut shredders currently in use that produce a residue particle size that does not exceed 1/32 inch in width by ½ inch in length may continue to be used for the destruction of classified information. Where maintenance is performed on such machines that involves rebuilding the shredder blade assembly, or, where new shredders are purchased for the destruction of classified information, the replacement or new purchase shall comply with CNSS Policy No. 16, National Policy for the Destruction of COMSEC Paper Material, and be equipment listed on the National Security Agency (NSA) Evaluated Products List (EPL) of High Security Crosscut Shredders. A copy of the EPL can be obtained by calling the NSA National Information Assurance Center at (800) 688-6115. Technical guidance on other methods of destruction can be obtained by contacting the JFO Security Officer.

9.1.3.
Technical guidance concerning appropriate methods, equipment, and standards for the destruction of classified electronic media, processing equipment components, and the like may be obtained by contacting the Directorate for Information Systems Security, National Security Agency, Ft. Meade, MD 20755.

10.0 Administrative Sanctions

10.1. Individual Responsibility

Any person who suspects or has knowledge of a violation, including the known or suspected loss or compromise of Classified National Security Information, shall promptly report the violation to the JFO Security Officer.

10.2. Violations Subject to Sanctions

Personnel are subject to administrative sanctions if they:

10.2.1.
Knowingly, willfully, or negligently disclose to unauthorized persons information classified under Executive Order 12958, Classified National Security Information, as amended, or its predecessor orders.

10.2.2.
Knowingly, willfully, or negligently violate any other provisions of Executive Order 12958, or knowingly and willfully grant eligibility for, or allow access to, classified information in violation of Executive Order 12958, as amended, or its implementing directives.

Tab 2 to Annex F: SOP for Verification of NSCI Clearances

1.0 Purpose

This Standard Operating Procedure (SOP) provides guidance on the security measures that will be implemented and adhered to for the verification of security clearances.

2.0 Applicability

This SOP applies to all personnel working in or around the Joint Field Office (JFO).

3.0 Individuals With Current Clearances

3.1. Verification

To verify an individual's clearance, the JFO Security Officer will either pass clearance information via fax or email, or access (via terminal or Internet) one or more of the following databases:

- OPM PIPS SII/Clearance Verification System (CVS) for civilian personnel;
- Joint Personnel Adjudication System (JPAS) for military personnel;
- Scattered Castles for individuals requiring access to SCI.

3.2.

Access to these databases may be available at FBI Field Office, DHS/USSS Field Office, military installation. Web-based versions are also available.

3.2.1.

If direct access to the above databases is not available, the JFO Security Officer will:

- Contact a DHS Security Office (via phone or email) with connectivity to the above databases. Security Offices include DHS HQ, CBP, TSA, USCG, DHS/USSS, DHS/FEMA, and ICE.
- Provide full name (includes middle name), Social Security Number (SSN), Date of Birth (DOB), Place of Birth (POB) to DHS Security Office; and
- Receive clearance verification (via phone, fax, email).

3.3.

Once the clearance has been verified via one of the above methods, the JFO Security Officer will issue access control card reflecting clearance level.

3.4.

The Office of Security will receive the FPS Security Officer cadre roster (DHS/USSS for NSSEs) and pre-clear these personnel for access to the Office of Security security database.

Tab 3 to Annex F: SOP for Emergency Disclosure of NSCI

1.0 Purpose

This Standard Operating Procedure (SOP) provides guidance on the security measures that will be implemented and adhered to for the disclosure of classified information to an individual or individuals who are otherwise not eligible for access.

2.0 Applicability

This SOP applies to all personnel working in or around the Joint Field Office (JFO).

3.0 Emergency Situations

In an emergency, and when necessary to respond to an imminent threat to life or in defense of the homeland, the Department Leadership Team may authorize the disclosure of classified information to an individual or individuals who are otherwise not eligible for access. Under these conditions, the approving official shall:

3.1.

Limit the amount of classified information disclosed and the number of individuals to whom it is disclosed to the absolute minimum necessary to achieve the intended purpose;

3.2.

Transmit the classified information via approved Federal Government channels by the most secure and expeditious method possible, or by other means deemed necessary when time is of the essence;

3.3.

Provide instructions about what specific information is classified and how it should be safeguarded. Physical custody of classified information must remain with an authorized Federal Government entity, in all but the most extraordinary and unique of circumstances;

3.4.

Provide appropriate briefings to the recipients on their responsibilities not to disclose the information and obtain a signed nondisclosure agreement. In emergency situations requiring immediate verbal release of information, the signed nondisclosure agreement memorializing the briefing may be received after the emergency abates;

3.5.
Within 72 hours of the disclosure of classified information, or the earliest opportunity that the emergency permits, but no later than 7 days after the release, the disclosing authority shall notify the DHS Chief Security Officer and the originating agency of the information. Such notification shall include:

- A description of the disclosed information;
- To whom the information was disclosed;
- How the information was disclosed and transmitted;
- Reason for the emergency release;
- How the information is being safeguarded; and
- A description of the briefings provided and a copy of the nondisclosure agreements signed.

3.6.
A copy of the signed nondisclosure agreements should be forwarded with the notification referenced in paragraph 3.5, above, or as soon thereafter as practical.

3.7.
Release of information pursuant to this authority does not constitute declassification thereof.

Tab 4 to Annex F: SOP for SCI/SCIF Operation

1.0 Purpose

This Standard Operating Procedure (SOP) provides guidance on the security measures that will be implemented and adhered to for the protection, use, and dissemination of Sensitive Compartmented Information (SCI).

2.0 Applicability

This SOP applies to all personnel working in or around a Joint Field Office (JFO) Sensitive Compartmented Information Facility (SCIF) accredited by the Department of Homeland Security. All persons authorized unescorted access to the JFO will read and be familiar with the requirements of this SOP.

3.0 Basic SCI Controls

Guidance concerning the control of SCI is contained in Director of Central Intelligence Directive (DCID) 6/1, "Security Policy for Sensitive Compartmented Information and Security Policy Manual." The following applies to the JFO SCIF:

3.1.

SCI material will only be disseminated on a need-to-know basis to individuals who hold the proper clearance level and access approval for the information. If the specific accesses of an individual are not known, the JFO Security Officer must verify the accesses prior to sharing information with that individual.

3.2.

SCI material may only be discussed, used, handled, electronically processed, or stored within an accredited Sensitive Compartmented Information Facility (SCIF).

4.0 Establishing a New Sensitive Compartmented Facility

The JFO shall request the establishment of a SCIF only when there are clear operational requirements and when existing SCIFs are not adequate to support the requirements. The JFO shall make use of existing SCIFs or consolidated SCIFs whenever possible.

4.1.

Physical security standards for the construction and protection of such facilities are prescribed in the current DCID 6/9, Physical Security Standards for Sensitive Compartmented Information. Procedures for establishing SCIFs are as follows:

4.1.1.

The requirements justifying a new SCIF shall be documented and maintained with accreditation records. When it is determined that a SCIF is necessary for the JFO, the JFO Security Officer will contact the DHS Office of Security and provide a Concept of Operations (CONOPS) document detailing the requirements for the SCIF establishment and a pre-construction, DCID 6/9, Fixed Facility Checklist, completed to the maximum

extent possible. The DHS Office of Security will provide assistance, as necessary, during this process in accordance with DCID 6/9.

4.1.2.
The DHS Office of Security shall ensure the SCIF is constructed in accordance with the security specification provided in DCID 6/9. Upon completion of construction, the Office of Security will ensure an inspection is conducted with qualified personnel to ensure it meets DCID 6/9 standards.

4.1.3.
The DHS Office of Security Chief will ensure Technical Surveillance Countermeasures (TSCM) inspections and TEMPEST inspections are conducted in accredited SCIFs, as necessary. The JFO Security Officer will coordinate requirements and consider mitigation strategies as necessary.

4.1.4.
The Central Intelligence Agency (CIA) or its designee will conduct a final inspection of the SCIF, and review and approve the required SCIF documentation and procedures. SCIF accreditation documentation will be approved by the Central Intelligence Agency or its designee.

4.1.5.
The JFO Security Officer shall obtain the approval of the CIA or its designee for any significant change affecting the integrity of any CIA-accredited SCIF, prior to any change in the SCIF construction or operating procedures. These may include, but are not limited to, changes in perimeter, alarms, or anything that might introduce a vulnerability to the facility.

5.0 Operational Contingencies
With prior DHS Senior Official of the Intelligence Community (SOIC) coordination, the DHS Chief Security Officer may approve temporary SCI accreditation not to exceed 180 days. The DHS Office of Security will assign a SCIF identification number and the DHS Chief Security Officer retains authority to cancel, extend, or modify any such accreditation.

5.1. Temporary Secure Working Areas
A temporary secure working area (TSWA) is a temporarily accredited SCI facility that is used no more than 40 hours monthly for handling, discussing, and/or processing SCI, but where SCI should not be stored. The “40 hours” is based on an average use of the TSWA over a 12-month period.

5.1.1.
During the entire period the TSWA is in use, the entrance will be controlled and access limited to persons having clearance for which the area has been approved. Approval for using such areas must be obtained from the Cognizant Security Authority (CSA) (the DHS Chief Security Officer) setting forth room number(s), building, location, purpose, and specific security measures employed during usage as well as during other periods.

5.1.2.
TSWAs should be covered by an alarm system. No special construction is required other than to meet sound attenuation requirements as set forth in Annex E of DCID 6/9, when applicable. If such a facility must also be used for the discussion of SCI, a Technical Surveillance Countermeasures (TSCM) evaluation may be required at the discretion of the CSA, as conditions warrant.

5.1.3.
When not in use at the SCI level, the TSWA will be:

- Secured with a keylock or a combination lock approved by the CSA.
- Access will be limited to personnel possessing a U.S. Secret clearance.
- If such a facility is not alarmed or properly protected during periods of non-use, a TSCM inspection may be conducted prior to use for discussion at the SCI level.

5.2. Tactical Facilities

The DHS Chief Security Officer may establish and grant temporary accreditation for tactical SCIFs, not to exceed 180 calendar days in one location. The DHS Chief Security Officer is responsible for a temporary field or tactical SCIF used in support of a JFO. Annex C to DCID 6/9 contains detailed policy, procedure, and physical security requirements for tactical SCIFs.

5.3. Declared Hostilities, General War, National Emergencies

During a period of declared hostilities, general war, or national emergency, a SCIF at any level of accreditation may be established by the JFO Security Officer upon the verbal order of the DHS Chief Security Officer or designee (General Officer/Flag Officer civilian equivalent level). Reconciliation of SCIF activation and operational data will be made not more than 180 days after SCIF activation. Interim reporting of SCIF activation may be made to Department of Homeland Security Office of Security where operationally feasible.

5.4. Semi-Permanent SCIFs

The DHS Chief Security Officer is the sole accrediting authority for nontactical Department of Homeland Security Semi-Permanent SCIFs (SPSCIFs). Requirements for TEMPEST and IT accreditation apply. Deployed SPSCIFs are considered tactical SCIFs and are under the authority of the Chief Security Officer.

6.0 SCI Computer Systems

SCI can be processed only on a computer, or network of computers, that has been specifically certified and accredited for that level of classified information.

6.1.

Telecommunications and automated information systems (TAIS) used to process, store, or handle SCI will be operated so that the information is protected against unauthorized disclosure, modification, access, use, destruction, or delay in service.

6.2.
All TAIS that process, store, or handle SCI will be certified and accredited by the DHS Designated Accreditation Authority (the Assistant Secretary for Information Analysis) prior to operation.

6.3.
All TAIS processing SCI will follow the requirements delineated in DCID 6/3.

6.4.
SCI systems will not be placed in operation until authorized, in writing, by the Designated Accreditation Authority.

7.0 Portable Electronic Devices
A portable electronic device (PED) is any non-stationary electronic apparatus with singular or multiple capabilities of recording, storing, processing, and/or transmitting data, video/photo images, and/or voice emanations. This definition generally includes, but is not limited to, laptops, PDAs, pocket PCs, palmtops, Media Players (MP3s), memory sticks (thumb drives), cellular telephones, PEDs with cellular phone capability, and pagers.

7.1.
The following procedures are to be followed for Government-furnished, mission-essential PEDs that are permitted in JFO SCIFs:

7.1.1.
Prior to entry, PEDs must be pre-approved by the JFO Security Officer with special consideration given to the PED's functionalities and mitigation requirements. Mitigation procedures for multi-function PEDs must address all of the functions associated with the device. Examples are PEDs with cellular phone, Infrared (IR), Radio Frequency (RF), or image-capturing capabilities.

Laptops with wireless capabilities may be brought into accredited SCI Facilities, provided the following guidelines are followed:

- Radio Frequency (RF): Laptops that have a wireless capability may be brought into and out of accredited SCIFs. However, the wireless functionality must be physically disabled. The RF capability may not be used at any time within the SCIF.
- Infrared (IR): Laptops that have an infrared capability may be brought into and out of accredited SCIFs. However, the IR port must be covered by metal tape while in the SCIF area. The IR capability may not be used at any time within the SCIF.

7.1.2.
Immediately upon approval and prior to use, PEDs must be registered with the JFO Security Officer via the "PED Registration Form," which may be obtained from the Security Officer.

7.1.3.
Users must adhere to all mitigation measures prescribed by the JFO Security Officer.

7.1.4.
Approval/registrations will be valid until the user transfers, terminates, or no longer has a need for the device; it is no longer essential to the DHS mission; or the user intends to make modifications that could affect the PED's security profile.

7.1.5.
The JFO Security Officer will affix a registration label/bar code that will be recognized by all DHS SCIFs as designating the PED acceptable for entry. PEDs must be appropriately labeled and controlled in accordance with applicable directives and regulations.

7.1.6.
Any person seeking to bring a PED into a DHS SCIF expressly consents to a random inspection of the PED and to its retention if it is suspected of containing classified information, or if the device is believed to have been compromised. In the event any PED is suspected of containing classified information without authorization, or if a PED is found to not be adhering to this directive, they are also subject to inspection by a forensics professional and/or retention by the U.S. Government. Any suspected illegal activities will be reported to the appropriate authorities for investigation.

7.1.7.
Any person approved to bring a PED into a DHS SCIF will be trained on the security requirements associated with the PED being introduced into the facility.

7.1.8.
Unclassified PEDs may not be connected, by any means, to any Information System that contains classified information.

7.1.9.
All requests for connecting PEDs within SCIFs must be approved by the JFO Security Officer. If connected to a classified information system, the PED must be controlled and classified to the highest level that the information system is accredited to process.

7.1.10.
Prior coordination with other government sites is required prior to introducing PEDs into their SCIFs.

8.0 Access

Access to any SCIF is a privilege, not a right, and the need-to-know for access to any SCIF by DHS personnel is determined by the JFO Security Officer.

8.1.

Access controls for a SCIF should be tailored to fit the local threat, the number of personnel requiring access, the geographic location of the SCIF, and the ability of the hosting organization to provide support. Visitors will be positively identified by photograph and Social Security number.

8.2.

All personnel who work in or have routine or unescorted access to SCIFs accredited for open storage or 24-hour continuous operations will be cleared and indoctrinated for the highest level of SCI authorized for that particular SCIF.

8.2.1.

Only permanent occupants are authorized unescorted or "badged" access to the SCIF.

8.2.2.

All SCI-cleared personnel not assigned to the SCIF are not authorized non-escort or "badged" access and must sign in and have their use of the SCIF monitored by permanent staff.

8.2.3.

If a SCIF has areas with different levels of SCI separated by an internal access control device, individuals will be indoctrinated at the highest level for which they are authorized unescorted access. Classify the associated door combinations and access codes at the highest level of SCI authorized for that particular area.

8.3. Access Rosters

Access rosters listing all persons authorized access to the facility will be maintained at or near the SCIF point of entry (within the SCIF). Electronic systems, including coded security identification cards or badges, may be used in lieu of security access rosters.

8.3.1.

Access rosters will contain the following data elements: name, office, Social Security number, Government agency, security clearance, and level of SCI access using only authorized digraphs/trigraphs (such as SI/TK). Access rosters are unclassified but will be marked as "For Official Use Only" and "Privacy Act Information."

8.3.2.

A Visitor Access Roster will be maintained for all other personnel, including other SCI-cleared personnel. The visitor log will include the following information: name of

visitor, organization, Social Security number, citizenship, purpose of visit, point of contact, and date/time of the visit. Escort is required for all personnel in this category.

8.4. Access Certifications

Certifications will include the person's full legal name; Social Security number; clearance level and SCI accesses required; dates of visit; purpose of visit; the name, telephone number, and the office symbol of the meeting point of contact at the visit location. The JFO Security Officer will classify the request as appropriate. The JFO Security Officer is responsible for requesting certifications only through DHS-approved channels and must consult Department of Homeland Security Special Security Officer (SSO) for guidance in the proper classification of visit/certification requests.

8.5. Non-Indoctrinated Personnel

DHS discourages SCIF access by non-SCI indoctrinated persons. SCIF personnel should conduct official business with non-indoctrinated visitors outside the SCIF. When it is necessary to grant access to non-indoctrinated person, an escort is required. Escort procedures are as follows:

8.5.1.

Escorts must inform and obtain clearance from the JFO Security Officer prior to bringing uncleared personnel into the SCIF. Escorts will inform the JFO Security Officer when the uncleared personnel have departed.

8.5.2.

Escorts should announce that an uncleared visitor is in the area, and notify personnel when the non-indoctrinated persons have departed. (A flashing or rotating red light is an excellent measure to indicate the continued presence of non-SCI indoctrinated personnel in the SCIF.)

8.5.2.1. Escorts are responsible for ensuring that co-workers turn over, cover, or store classified material; walk with the individual under escort; and visually observe the individual under escort until the visitor leaves the SCIF or another escort assumes the duty.

8.5.2.2. Escorts are responsible for ensuring that escorted individuals have relinquished all prohibited items prior to entry.

8.6. Access to SCIFs by Foreign Nationals

Visits or other entry into DHS SCIFs by non-U.S. citizens (including U.S. resident aliens or "Green Card" holders) is PROHIBITED.

9.0 Inspections and Baggage Checks

The purpose of the inspection is to prevent the introduction of unauthorized items into SCIF spaces and to prevent the unauthorized removal of Government property and classified materials.

9.1.
Such checks may include, but are not limited to, briefcases, newspapers, notebooks, magazines, gym bags, and other such items. Although this practice may involve some inconvenience, the inconvenience can be considerably reduced if the number of personal articles taken into or remove from the SCIF is minimized.

9.2.
All SCIF work areas and equipment are also subject to inspection for security, health, safety, and other official purposes. Items subject to inspection by DHS SSO or designees include, but are not limited to, computers, computer equipment and discs, safes, desks, file cabinets, bookcases, and other storage facilities. All items present in a SCIF are subject to being seized, inspected, and analyzed or read. Evidence of regulatory or legal misconduct will be subject to review and action by administrative and/or legal authorities.

9.3.
Individuals removing property from DHS SCIFs must have a property pass and the appropriate equipment/media form issued by authorized DHS SSO personnel.

10.0 Controlled Items
The following Government items may be brought into or removed from a DHS-accredited JFO SCIF only when absolutely necessary and upon security review and approval of the JFO Security Officer:

10.1.
Equipment for air quality testing, measuring of radio frequency of ionizing radiation, devices for life-safety purposes, and systems that are installed for a transitory purpose to ensure the security or safety of SCIF personnel or the physical integrity of the structure.

10.2. Emergency Personnel and Equipment
Emergency and Police personnel and their equipment, including devices carried by Emergency Medical personnel responding to a medical crisis within a SCIF, shall be instantly admitted to the SCIF without regard to their security clearance status. Emergency personnel will be escorted if practical.

11.0 Prohibited Items
A number of items cannot be brought into DHS SCIFs because of potential security or safety hazards.

11.1. Prohibited Items:

- Firearms or weapons of any type, ammunition, and explosive devices. Armed Guard Force personnel may enter the SCIF with their weapon ONLY when responding to an alarm condition, panic switch call, or reported threat.
- Devices that use Bluetooth wireless technology.

- Devices that have audio, video, or recording capabilities.
- Government-Furnished and/or personally owned Personal Digital Assistants (PDAs).
- Government-furnished and/or personally owned cellular phones.
- Pagers and beepers with the exception of government-furnished receive-only pagers.
- Personally owned laptops and notebook computers.

12.0 Storage

SCI material will be maintained and stored in a SCI-approved and accredited SCIF.

12.1.

Combinations should be given to a limited number of SCI indoctrinated personnel consistent with effective SCIF operations. Change COMSEC combinations according to COMSEC regulations. Combinations to locks installed on security containers, perimeter doors, windows, and any other openings should be changed when:

- A combination is first installed or used.
- A combination has been subjected, or believed to have been subjected, to compromise.
- At other times when considered necessary by the JFO Security Officer.

12.2.

SCI material may be filed in any manner meeting retrieval requirements. SCI material should be segregated from other material in a separate file cabinet, drawer, or folder. Security regulations or directives governing collateral files do not apply to SCI material.

12.3.

SCI when not in a storage status will be covered, turned face down, or otherwise protected when unauthorized persons are present, and returned to approved storage containers as soon as practicable.

13.0 Information Security

The author or drafter of a document is responsible for properly complying with established security classification guidance and for properly applying that guidance to a document, including all markings required for its protection, control, and dissemination. All personnel who produce, transmit, reproduce, or extract SCI from documents or other material must ensure the resulting SCI product is properly marked and protected. Protect all working materials such as drafts, computer disks, and typewriter ribbons in the same manner as the final material. Report errors in classification and marking, control, or dissemination problems to the responsible SCI security official.

14.0 Accountability

SCI material is non-accountable except material specifically designated as “accountable SCI.”

14.1.

SCI security officials responsible for SCIFs will maintain manual or electronic records of external receipt and dispatch sufficient to investigate loss or compromises of all SCI documents during transmittal. Users of SCI should use administrative/correspondence control numbers for ease in tracking and identifying documents.

14.2. Non-accountable SCI

Non-accountable SCI is SCI material that does not required document accountability (i.e., document accountability numbers, copy numbers, annual inventory, and Certificates of Destruction). SI/TK/G and Secret BYE material has been designated as non-accountable SCI. Non-accountable SCI must be controlled for need-to-know and transmission purposes.

14.3. Accountable SCI

Accountable SCI is SCI determined by the DCI or designated program Executive Agent to be of such critical sensitivity as to require the most stringent protection methods, including traceability and audit. Top Secret BYE has been designated as accountable SCI. An annual report of accountable authorizations, volume, and cost may be required at the request of the DCI.

14.4. Accountability Records

Accountability records are not required for non-accountable SCI. Raw intelligence (collected intelligence information that has not yet been converted into finished Intelligence) is considered non-accountable SCI.

14.5. Incoming Accountable SCI

A record will be kept of accountable SCI documents received by a SCIF. Records will identify the material by document accountability number (DAN) and copy number, originator, a brief description of the material, and the identity of the office(s) within the SCIF receiving the material. Keeping copies of receipts or maintaining other records that provide required identifying data will satisfy this requirement. For electronically received record traffic, retention of standard telecommunications center records will fulfill this requirement. No further records or administrative controls (e.g., internal receipting among activities in the same SCIF and access records) are required while SCI documents are maintained in or accountable to a receiving SCIF.

14.6. Outgoing Accountable SCI

A receipt, manual, electronic, or equivalent record, is required for accountable SCI dispatched from the SCIF. Receipts will identify the material by DAN, copy number, and originator; contain a brief description of the material; and identify the recipient. For Confidential SI-related material, the required Defense Courier Service (DCS) pouch or package receipt or by other appropriate dissemination records kept by the sender may fulfill this requirement. The dispatching SCIF is responsible for preparing receipts for SCI material.

14.6.1.
Assign a DAN to accountable SCI material only. DANs are not required for SI/TK/G or Secret/BYE documents.

14.6.2.
The designated document control officer assigns DANs. The numbers consist of the identifying trigraph, a 6-digit number on a one-up basis, and the last 2 digits of the current year, separated by a hyphen (e.g., BYE-000235-97). Place a DAN in the designated block on the cover sheet and on the front cover (if any), the title page (if any), and on all succeeding pages in the lower right corner.

14.6.3.
Assign copy numbers to individual documents (e.g., Copy 1 of 3 copies). Place the copy number next to or near the control number at the lower right corner of the document. Show reproduced copies with a combination of digits and letters (i.e., Copy 1A, Copy 4C, etc.) or identify the copy as Series B, Series C, etc.

14.7. Records Retention
For accountable SCI, retain records of incoming and outgoing accountable SCI (such as receipts and document control logs) and certificates of destruction as permanent records. For non-accountable SCI, transmission receipts may be destroyed on acknowledgment of successful transmission to the intended recipient.

15.0 Transportation and Transmission of SCI Material
In developing SCI material, give primary consideration to the intended use of the information and organize the document, if possible, so that SCI can be disseminated separately on a more limited basis, such as an annex or supplement. Review the document before final production to ensure that only the minimum scope and level of information essential to the task are included.

15.1.
SCI materials sent between accredited SCIFs will be hand-carried by individuals who are properly briefed on courier procedures, possess a valid courier card or letter, and who are cleared for the material being transported. SCI material will not be sent to a facility or building that does not have a SCIF, nor to an individual who does not have access to a SCIF.

15.1.1. Courier Requirements
Couriers will be a U.S. Government civilian employee, or a DHS contractor or consultant. Couriers will meet DCID 6/4 standards, be specifically designated as a courier, and have authorized access to the SCI material they are transporting or hold a PROXIMITY access. They must be familiar with all rules and regulations governing couriers and transporting information, including hand-carrying aboard commercial or private aircraft. SCI material will be properly wrapped prior to giving the material to a courier with a proximity access.

15.1.2. Issuing Courier Letters to Non-assigned Personnel

Local SCI security officials may issue courier letters of authorization to non-assigned personnel to hand-carry SCI under the following conditions:

15.1.2.1. The local SCI security official verifies the individual has the appropriate clearance and access level.

15.1.2.2. The parent or supporting SCI security office confirms the requirement for the individual to courier the material. The confirmation may be by telephone.

15.1.2.3. The local SCI security official packages the material and prepares the proper receipts and inventory list.

15.1.3.
Materials carried within a building should be in a sealed opaque envelope that is properly addressed.

15.1.4.
SCI shall be enclosed for shipment in two opaque envelopes or be otherwise suitably double-wrapped using approved containers.

15.1.5.
Outer containers shall be secured by an approved means that reasonably protects against surreptitious access. The inner and outer containers shall be annotated to show the package number and addresses of the sending and receiving SCIF. The notation "TO BE OPENED BY THE (appropriate SCI Special Security Officer)" shall be placed above the pouch address of the receiving SCIF on the inner container. The inner wrapper shall contain the document receipt and name of the person or activity for which the material is intended. The applicable security classification and the legend "CONTAINS SENSITIVE COMPARTMENTED INFORMATION" shall appear on each side of the inner wrapper only.

15.1.6.
Materials transported between buildings will be double-wrapped in the same manner required for National Security Information.

15.1.7.
SCI materials may be electronically transferred between appropriately accredited machines (facsimile, computers, secure voice, secure e-mail, or any other means of telecommunication ensuring that such transmissions are made only to authorized recipients). It is essential to ensure that appropriate secure devices are used for any type transfer of SCI material.

15.1.7.1. Facsimile Control Procedures

- SCI documents transmitted by secure facsimile will be marked, controlled, and accounted for in the same manner as hardcopy documents.

- Individual header or cover sheets used to precede the transmission of SCI material by secure facsimile will be conspicuously marked with the highest security classification of the transmitted material and unclassified digraphs/trigraphs, handling caveats, and DCID 6/6 control markings. The cover sheet will include the originator's name, organization, and phone number; a brief description of the SCI or subject; the classification; the number of pages; and the receiver's name, organization, and phone number, and a portion requesting the name, organization, and phone number of the receiver.

- For accountable SCI documents, the receiver will complete the receipt portion of the cover sheet and immediately retransmit the cover sheet to the sender.

15.1.7.2. Temporary release outside a SCIF. If operational needs require SCI to be released for accessing or temporary use by SCI-indoctrinated persons in non-SCI accredited areas, only the responsible SCI security official may grant such release. The responsible officer will obtain signed receipts for SCI released in this manner and will ensure that conditions of use of the released material provide adequate security until the SCI is returned to a SCIF by the end of the duty day. If used in a 24-hour operation, the SCI material must be sighted by the responsible SCI security official at least once every 24 hours. SCI material contained in a locked or sealed courier pouch or other container may not be left with non-SCI indoctrinated personnel. This does not include transmission of properly wrapped SCI by DCS or U.S. Diplomatic Courier Service personnel.

15.1.7.3. Any loss, compromise, or suspected compromise of SCI materials will be immediately reported to the JFO Security Officer.

16.0 Reproduction

Reproduction of SCI documents will be kept to a minimum consistent with operational necessity. SCI will be reproduced in a SCIF on equipment designated and matted for the reproduction of SCI. Post notices prohibiting the reproduction of SCI on equipment used for reproduction of collateral or unclassified information.

16.1.

Stated prohibitions or limitations against reproduction will be honored. The originator is the approval authority for reproduction in such cases. Only the organizational SCI security official, designee, or originator may authorize reproduction of Gamma or BYE material.

16.2.
Copies of documents are subject to the same control, accountability, and destruction procedures as the original documents. Extracts of documents will be matted according to content and treated as working materials.

16.3.
Equipment that leaves latent images in the equipment or on other material or that has the capability to connect to remote diagnostic centers, such as by telephone lines, is prohibited for SCI reproduction.

17.0 Disposition and Destruction

17.1.
SCI will be retained for the time periods specified in records control schedules approved by the Archivist of the United States (44 U.S.C. 3302 and FPMR 101-11.4). Destroy duplicate and non-record copies of SCI documents as soon as their purpose has been served.

17.2.
Destroy SCI in a manner that will prevent reconstruction. Only those DCI-approved methods (e.g., burning, pulping, shredding, pulverizing, melting, or chemical decomposition, depending on the type of materials to be destroyed) may be used. Appropriately indoctrinated person(s) will conduct the destruction.

17.3.
Destruction certificates are required for accountable SCI. If an organization maintains a master record of accountable SCI and destruction is recorded in the master record, individual destruction certificates may be destroyed after recording in the master record. Microfiche copies of accountable records are authorized provided all information is readable and hardcopy prints can be made to meet investigative or judicial requirements.

17.4.
SCI in computer, IT application, or other magnetic media will be destroyed as specified in the "Guide to Understanding Data Remanence in Automated Information Systems," (NCSC-TG-025) September 1991, or successor publication or as authorized by NSA in other publications.

17.5.
If burn bags are used to hold SCI waste, mark the bag when placed in use with the highest security classification of the material it might contain, the phrase "CONTAINS SCI MATERIAL," and the office symbol and phone number of the SCIF. When filled, seal the bag with staples or tape to prevent accidental tearing or breaking. In SCIFs not accredited for open storage, SCI waste must be secured in approved GSA security containers.

18.0 End-of-Day Procedures

The JFO Security Officer will establish a system of written security checks at the close of each working day to ensure the SCIF is secure. Standard Form 701, "Activity Security Checklist," will be used to record such checks. An integral part of the security check system will be securing of the SCIF, vaults, and containers used for the storage of classified material. Standard Form 702, "Security Container Check Sheet," will be used to record securing actions. Forms 701 and 702 are never to be placed on the outside/public side of a SCIF entrance door. These forms should be placed on the SCIF interior side of the door. Standard Forms 701 and 702 will be annotated to reflect after-hours, weekend, and holiday activity. Retain both forms for one year after completion or as required for investigative purposes.

18.1.

The individual assigned to conduct the security double check for the day will check the following items (as required):

- Double check Standard Forms 702 to ensure all appropriate entries for locking and checking have been made for each security container.
- Double check desk tops, cabinets and safe tops, shelves, stands, tables, and other furniture and equipment for unsecured classified material.
- Double check wastebaskets for classified material. Ensure that all burn bags are properly secured.
- Double check typewriters to ensure that all typewriter ribbons used in the preparation of classified material have been removed and secured.
- Double check IT, word processing, or recording equipment to ensure that all recording media have been removed and properly stored.
- Double check charts, maps, blackboards, clipboards, and other items hanging on the walls that might contain classified information.
- If applicable, double check all windows and access to ensure they are properly secured.
- Double check the intrusion detection system, if applicable, to ensure that it is properly set and activated.
- Double check other items on SF 701. Initial the form when checks are completed.
- Check SF 702 at the SCIF entrance to ensure that the "locked by" and "checked by" columns have been completed. Recheck the door to ensure it is locked.
- Ensure that the SF-702 is located INSIDE the SCIF for OPSEC purposes.

19.0 Security Violations

Security protection of SCI control systems and related products and material is paramount. All actual or suspected incidents of the compromise of SCI will be immediately investigated.

19.1. Security Violation

A security violation is a compromise of classified information to persons not authorized to receive it or a serious failure to comply with the provisions of Security regulations or this SOP, which is likely to result in compromise. A security violation requires investigation.

19.2.

Violations can result from, but are not limited to, deliberate or accidental exposure of SCI resulting from loss, theft, or capture; recovery by salvage; defection; press leaks or public declarations; release of unauthorized publications; or other unauthorized means.

19.3.

Loss or exposure of SCI from any cause requires immediate reporting, investigation, and submission of a damage assessment describing the impact on national security.

19.4. Practice Dangerous to Security (PDS)

A PDS is a failure to comply with the provisions of security regulations or this SOP, which causes a potential compromise of classified information.

- A PDS requires immediate action but does not require investigation. A PDS does not constitute a security violation but can lead to security violations or compromises if left uncorrected. Examples of PDS include, but are not limited to, a courier carrying classified documents stopping at a public establishment to conduct personal business, placing burn bags adjacent to unclassified trash containers, or failing to change security container combinations as required.
- Report all security incidents to the JFO security official.

20.0 Emergency Action Plans

The JFO SCIF will establish and maintain an emergency action plan (EAP). The plan may be part of an overall department, agency, or installation/facility plan as long as it satisfactorily addresses the considerations stated below. The JFO Security Officer is responsible for the EAP.

20.1. Requirements for all EAPs

All EAPs will include the following:

- Location of fire-fighting equipment.
- Assignment of specific responsibilities by duty position, rather than by name, with alternates designated.
- Authorization for the senior individual present to implement the plan.
- Periodic review of assigned duties by all personnel.
- Location of SCI material by storage container.
- Location of safe combinations.

- Procedures for admitting uncleared emergency personnel into the SCIF and provisions for safeguarding SCI material during such access.
- Removal of SCI document accounting records to facilitate the post-emergency inventory.
- Emergency evacuation procedures for equipment, material, and personnel, as appropriate.
- Emergency storage procedures, if appropriate.
- Provisions for precautionary and complete destruction, if appropriate.
- Designation of evacuation site and alternate site.
- Designation of primary and alternate travel routes.
- Provision of packing, loading, transporting, and safeguarding SCI material.

20.2.

Evacuation will be executed in a systematic manner under the direction of a responsible individual. Every effort will be made to prevent loss or unauthorized viewing of SCI until the return of the information to its original location or the SCI is relocated to an alternate SCIF. Factors that may influence the decision to evacuate the SCIF include the following:

- Time available.
- Future requirement for the SCI material.
- Degree of hazard involved in the removal.
- Safety of the new location.
- Means of transportation available.
- Transportation routes available.

20.3.

When implementation of emergency plans results in abandonment of SCI material, the DHS SSO or Chief Security Officer will ensure that every reasonable effort will be made to recover the material as soon as possible. Recovery will be based on the likelihood of success without subjecting personnel to undue danger. SCI or residue will be collected and placed under the control of SCI-indoctrinated individuals until disposition instructions are received.

20.4. Secure Storage

Secure storage consists of securing the SCI material in other SCIFs or safes before evacuating the area. Presence of a guard does not satisfy secure storage requirements; however, placement of guards by stored material is required when possible. Factors that may influence the decision to secure the SCI area include:

- Time available.
- Nature of the emergency (whether by human or natural causes).
- Seriousness of the emergency.
- Likelihood of returning to the site.
- Bulk or weight of the material (in deciding whether to store or evacuate).

20.5. Destruction

Material will be identified for emergency destruction/removal according to the following priority:

20.5.1. Priority One

All cryptographic equipment and documents.

20.5.2. Priority Two

All operational SCI codeword material that might divulge targets and successes, documents dealing with U.S. SCI activities, and documents concerning compartmented projects and other sensitive intelligence materials and TOP SECRET collateral.

20.5.3. Priority Three

Less sensitive administrative SCI material and collateral classified material not included above.

20.5.4.

Selection of an adequate destruction method should be based on a comprehensive evaluation of conditions at a specific SCIF. Destruction of SCI equipment should be by one of the following means.

- Acetylene torches.
- Incendiaries.
- Although not as effective, destruction or disassembling, smashing, or scattering components may be accomplished when incendiaries or acetylene torches are not available. Equipment also may be jettisoned into water deep enough to minimize the possibility of salvage.
- Documents and other flammable material may be destroyed by burning. Kerosene, gasoline, and sodium nitrate are effective means of destroying documents. They should be used with extreme care for personal safety. Documents also may be destroyed by:
  - Pulverizing.
  - Pulping.
  - Enclosing in a weighted, perforated bag, and jettisoning into water deep enough to minimize the possibility of recovery.

20.6. After Action Report

The actions listed below are required after initiation of EAPs.

20.6.1.

The JFO Security Officer will submit a written report as soon as possible to the DHS Chief Security Officer.

20.6.2.

Reports will, as a minimum, indicate the following:

- Material destroyed and method used.
- Circumstances that caused the plan to be implemented.

20.7.

Emergency plans will be reviewed annually and updated as necessary. All personnel shall be familiar with the plans.

21.0 Closeout Guidelines

- Inspect storage containers and furniture. Remove and inspect each drawer, leaf, or part, including areas under drawers and cushions or other parts that might conceal classified material. Ensure the container or furniture does not contain classified, official, or Government-related material.

- Reset combination safes to the manufacturer's setting of 50-25-50 and lock them.

- Lock key-lockable containers and tape the key to the drawer or door handle.

- Affix a certification form (may be locally produced) that reflects the date of inspection, name and signature of inspector, and a statement that the inspector certifies that classified, official, or Government-related material is not contained therein. Remove the form when the item is reissued or release outside the agency.

- Remove typewriter and printer ribbons and dispose of them as SCI material.

- Ensure reproduction equipment does not contain classified information or latent images of such.

- Dispose of SCI equipment and media, including hard drives and portable storage media, according to approved procedures and request withdrawal of IT security accreditation.

- Inspect entire SCIF to ensure all SCI material has been removed, properly disposed of, or destroyed.

- Request accreditation withdrawal from accreditation authority.

- Receive formal withdrawal from accreditation authority.

- If facility will be used for another mission or project that requires alarms, transfer alarm service to the new activity. If facility will not be used for another mission or project, discontinue the alarm service, including removal of alarms and the wiring system.

- If applicable, change the combination on the entrance door to 50-25-50, and account for all keys.

- Debrief personnel, if required.

Tab 5 to Annex F: Template Physical and Information Security Plan

[RESERVED]

Tab 6 to Annex F: SOP for SBU Information Handling

1.0 Definition

FOUO (For Official Use Only) is the designator used within DHS to identify sensitive but unclassified information within the DHS community that is not otherwise specifically described and governed by statute or regulation. FOUO provides for a level of protection not afforded other types of unclassified information.

1.1

DHS has three types of sensitive but unclassified information: FOUO, SSI, and PCII. FOUO, the focus of this SOP, is the most common and is governed by DHS Management Directive (MD) 11042.1. Sensitive Security Information (SSI) is sensitive but unclassified information used for certain types of TSA and Coast Guard information, which is governed by 49 CFR Part 1520. Protected Critical Infrastructure Information (PCII) is also used within DHS to indicate certain types of information associated with critical infrastructure vulnerabilities. PCII is governed by 6 CFR Part 29.

1.2

Other Federal departments and agencies use other markings besides FOUO to indicate that information is sensitive but unclassified. A partial listing is provided at the end of this SOP. Generally, unless instructed otherwise by the originator, other department and agency products that are sensitive but unclassified can be protected, transmitted, and destroyed in accordance with MD 11042.1. Refer to the listing at the end of this SOP for types of information that warrant protections beyond those for FOUO.

2.0 Designation

Any DHS employee, detailee, or contractor can designate information as FOUO provided it falls within one of the eleven categories of information listed in the MD as FOUO. Officials occupying supervisory or managerial positions are authorized to designate other information, not listed in the MD and originating under their jurisdiction, as FOUO.

2.1

The categories of information that can be designated FOUO are as follows:

- Information exempt from disclosure under the Freedom of Information Act (FOIA)
- Information exempt from disclosure under the Privacy Act
- Information within the banking and financial communities protected by statute, treaty, or other agreements
- Other international or domestic information protected by statue, treaty, or other agreements
- Information that could be sold for profit
- Information that could result in physical risk to personnel
- DHS information technology internal systems data
- System security data revealing the security posture of a system
- Reviews or reports illustrating or disclosing facility infrastructure or security

vulnerabilities
- Information that could constitute an indicator of U.S. Government intentions, capabilities, operations, activities, or otherwise threaten operations security
- Developing or current technology information, the release of which could hinder DHS objectives or compromise an advantage or countermeasure.

3.0 Marking

Information designated as FOUO will be sufficiently marked so that persons having access to it are aware of its sensitivity and protection requirements. At a minimum, prominently mark on the bottom of each page "FOR OFFICIAL USE ONLY." Materials containing specifics types of FOUO information may be further marked with an applicable caveat, e.g., "LAW ENFORCEMENT SENSITIVE," in order to alert the reader to the type of information conveyed. Additional access and dissemination restrictions may also be cited as the situation warrants.

3.1

Portion markings (i.e., markings within a document applicable to individual chapters, sections, paragraphs, or lines) are not normally required unless FOUO is used in a classified document. However, portion markings may be applied at the discretion of the originator to distinguish FOUO information from information that is not sensitive. When portion markings for FOUO information are used they shall be annotated as "(FOUO)" and applied at the beginning of the portion or paragraph.

3.2

Designator or originator information and markings, downgrading instructions, and date/event markings are not required on FOUO documents.

4.0 Handling/Storage

When unattended, FOUO information will be stored in a locked filing cabinet, locked desk drawer, a locked overhead storage compartment such as systems furniture credenza, or a similar locked compartment.

4.1

FOUO information can also be stored in a room or area that has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without a need-to-know, such as a locked room or an area where access is controlled by a guard, cipher lock, or card reader.

4.2

No clearance is needed for access to FOUO information; however, there has to be a 'need to know'.

4.3

FOUO information shall not be posted on public websites.

5.0 Transmittal

Use of secure phone and faxes for transmittal of FOUO information, although not required, is encouraged.

5.1

When feasible, FOUO should be transmitted through secure, encrypted email channels. However, when this is impractical or unavailable, FOUO may be transmitted over regular email channels. Password protection of FOUO attachments should be considered. Do not send FOUO email to a personal email account.

6.0 Destruction

Hard copy FOUO materials will be destroyed by shredding, burning, pulping, or pulverizing, sufficient to assure destruction beyond recognition & reconstruction.

6.1

After destruction, FOUO materials may be disposed of with normal waste.

6.2

FOUO electronic storage media shall be sanitized appropriately by overwriting or degaussing.

6.3

Paper products or electronic media containing FOUO information will not be disposed of in regular trash or recycling receptacles unless the materials have first been destroyed as specified above.

7.0 Violations

FOUO incidents on DHS IT Systems will be reported to the Organizational Element's Computer Security Incident Response Center.

7.1

Suspicious or inappropriate requests for information shall be reported to the DHS Office of Security.

7.2

At the originator's request, an inquiry will be conducted by the servicing Security Official or other Designee.

8.0 Assistance

DHS Office of Security Customer Service Center: (202) 692-4432.

Common Markings Used for Sensitive but Unclassified Information

INITIALS	MEANING	HANDLING REMARKS
DSEN	Drug Enforcement Agency Sensitive	Similar to FOUO. Destroy in same manner as CONFIDENTIAL. Contact a DEA representative
FOUO	For Official Use Only	Used by DHS, DOD, and other agencies.
LES	Law Enforcement Sensitive	Similar to FOUO.
LIMDIS	Limited Distribution	Used by National Geospatial-Intelligence Agency. Restrictions apply. Contact an NGA representative.
LOU	Limited Official Use	Used by Department of Justice. Similar to FOUO.
OUO	Official Use Only	Used by Department of Energy. Restrictions apply. Contact a DOE representative.
PCII	Protected Critical Infrastructure Information	Used by DHS. Restrictions apply. Contact the DHS PCII Program Office.
PROPIN	Proprietary Information	Restrictions apply. Contact the originator.
SBU	Sensitive But Unclassified	Used by Department of State and other agencies. Similar to FOUO.
SGI	Safeguards Information	Used by the Nuclear Regulatory Commission. Restrictions apply. Treat as CONFIDENTIAL. Contact an NRC representative.
SSI	Sensitive Security Information	Used by DHS and Department of Transportation for sensitive information within the transportation sector Restrictions apply. Contact a TSA or US Coast Guard representative.
SSI	Sensitive Security Information	Used by Department of Agriculture for information under their purview. Similar to FOUO.
UCNI	Unclassified Controlled Nuclear Information	Used by DOD/DOE. Restrictions apply. Contact a DOD or DOE representative.

Annex G: Principal Federal Official

1.0 Alert and Designation

1.1 Pre-Designation

In certain scenarios, a PFO may be pre-designated by the Secretary of Homeland Security to facilitate Federal domestic incident planning and coordination at the local level outside the context of a specific threat or incident. A PFO may also be designated in a pre-incident mode for a specific geographic area based on threat and other considerations. See Tab 1 to this Annex for the Warning Order used in these situations.

1.2 Designation

The Secretary of Homeland Security may, at his or her discretion, designate a PFO for an Incident of National Significance, to include a cadre of pre-identified individuals around the United States trained to perform the PFO function; the Secretary may select from among this cadre at his or her discretion. See Section 4.3.1 of this SOP for a discussion of the Initiation Process.

- The Secretary may designate an interim PFO for the incident until a primary designated PFO is in place. This interim PFO will perform all of the PFO's functions until relieved by the designated PFO.
- Upon designation, the Secretary will direct the HSOC to notify all internal DHS watch centers and other Federal operations centers, as well as appropriate State, tribal, local, regional, and nongovernmental EOCs and relevant elements of the private sector. The DHS Office of Public Affairs will normally prepare a press release and/or press conference.
- Internal DHS watch centers will initiate appropriate notifications. The HSOC/NRCC will notify NRP agencies and activate NRP teams and facilities.
- The SIOC will have responsibility for all FBI notifications regarding the PFO designation.
- In the event that the DEST deploys, the PFO may accompany the DEST to the incident site. See Tab 9 to this Annex.

2.0 Roles and Responsibilities

The specific roles and responsibilities of the PFO include the following:

- Representing the Secretary of Homeland Security locally as the lead Federal official;
- Ensuring overall coordination of Federal domestic incident management and resource allocation activities;
- Ensuring seamless integration of Federal activities in support of and in coordination with State, local, and tribal requirements;
- Providing strategic guidance to Federal entities;
- Facilitating interagency conflict resolution as necessary;

- Serving as a primary, although not exclusive, point of contact for Federal interface with State, local, and tribal senior elected/appointed officials, the media, and the private sector;
- Providing real-time incident information to the Secretary of Homeland Security through the HSOC and the IIMG, as required;
- Coordinating response resource needs between multiple incidents as necessary, or as directed by the Secretary of Homeland Security;
- Coordinating the overall Federal strategy locally to ensure consistency of Federal interagency communications to the public;
- Ensuring that adequate connectivity is maintained between the JFO and the HSOC; local, county, State, and regional EOCs; nongovernmental EOCs; and relevant elements of the private sector; and
- Participating in ongoing steady-state preparedness efforts, as appropriate for PFOs designated in a "pre-incident" mode, when a threat can be ascribed to a particular geographic area.

3.0 Concept of Operations

3.1 Task Organization

3.1.1 General

The PFO will be supported by a small staff of personnel from DHS and non-DHS agencies and departments, referred to as the PFO support staff. Using the scalable organizational structure of the NIMS in the context of both pre-incident and post-incident activities, other elements and staffs may be attached to the PFO support staff during the initial phases of Incident Management. While the PFO will retain the PFO support staff (except the Chief of Staff), the liaisons and other subject-matter expert staff attached to the PFO support staff will move into the appropriate ESF or JFO Coordination Staff (where no appropriate ESF has been activated) once the JFO is established. When traveling, the PFO will be supported by appropriately scaled advance and security elements.

3.1.2 PFO Support Staff

The PFO support staff will be comprised of the following: the PFO, Deputy PFO, Chief of Staff, Operations Officer, HSOC Representative, and Press Secretary. The PFO support staff will be an important element of the initial JFO. When the JFO scales up, the Chief of Staff moves to lead the JFO Coordination Staff in support of the entire JFO Coordination Group.

3.1.2.1 Deputies and Personal Staff

Deputy Principal Federal Official. The Deputy PFO operates under the authority and direction of the PFO. The Deputy PFO generally manages the staff on behalf of the PFO to achieve the Secretary's intent, freeing the PFO to interact with the appropriate agencies and be present at critical times and places to oversee incident management. The Deputy PFO responsibilities include, but are not limited to:

- Provides guidance to the PFO support staff and resolves any issues involving priorities or use of internal resources;
- Coordinates with the PFO to ensure that the Secretary's intent is followed;
- In the absence of the PFO, manages the PFO support staff in accordance with Secretarial intent;
- When delegated by the PFO, serves as a Federal interface to State, local, and tribal officials, the media, and the private sector; and
- Oversees the daily preparation of SITREPs and other reports as required or directed.

Chief of Staff

- Assists the PFO and Deputy PFO, as required, in the execution of the responsibilities outlined above;
- Provides guidance to the PFO support staff and resolves issues involving priorities or use of internal resources;
- Coordinates PFO support staff movements;
- Coordinates briefings, visits, and tours by high-level government officials, Members of Congress, and dignitaries;
- Coordinates logistical and security support for the PFO and PFO support staff; and
- Oversee tracking of the financial resource requirements of the incident response effort.

Operations Officer

- Supports the PFO, Deputy PFO and the Chief of Staff in the execution of their responsibilities;
- Serves as the primary point of contact for pre-deployment administration and logistics support of the PFO support staff and host Federal, State, or local agencies;
- Facilitates initial in-brief of team members upon activation of the PFO support staff;
- Assists the PFO/Deputy PFO and Chief of Staff with planning, coordination, and/or liaison tasks, as assigned;
- Supervises the daily development and distribution of SITREPs and other reporting requirements by assigned HSOC personnel;
- Provides direct reach back to IMD operations and planning subject-matter expertise, in support of the PFO/Deputy PFO requirements;
- Provides the PFO and the Director, IMD overarching observations related to enhancing facilitation of interagency prevention, protection, preparedness, and response coordination; and
- Captures items/issues and develops the After Action Report (AAR).

Administrative Assistant. Staff representatives from selected directorates will serve as recorders for the PFO; specific requirements will vary depending on the nature of the incident. These recorders represent the Planning Section and facilitate the collection, evaluation and dissemination of information about the incident and use of resources. The completeness and accuracy of records may be critical to documenting the need for State and/or Federal assistance and also may be critical should an event occur that results in future litigation. Additional responsibilities include the following:

- Assists the Deputy PFO in tracking the financial resource requirements of the incident response effort;
- Serves as the primary collectors for after-action issues;
- Ensures that the JFO Situation Unit receives timely and accurate information for the preparation of SITREPs as required; and
- Assists the PFO support staff Operations Officer in pre-deployment administration, travel, and logistical support to the PFO support staff.

Information Analysis Intelligence Analyst. Responsible for providing daily intelligence updates to the PFO and PFO support staff members regarding current intelligence relating to the incident and/or threat obtained from the DHS Office of Intelligence & Analysis, FBI, local law enforcement, and other relevant incoming information/intelligence sources. Additional responsibilities include the following:

- Provides direct reach-back to DHS Office of Intelligence & Analysis to provide PFO access to its Morning Executive Briefings and other daily briefings, subject-matter experts, and access to pertinent analytical products and threat advisories;
- Conducts daily conference calls with Office of Intelligence & Analysis leadership to discuss current intelligence;
- Provides presence in the JFO to ensure PFO connectivity with the Chief Intelligence Officer regarding intelligence matters. If the PFO relocates to any other location, the senior Office of Intelligence & Analysis liaison will travel with the PFO as his/her intelligence representative;
- Assists the PFO with information gathering and analysis; and
- Provides daily input to the PFO SITREP and other reports as required or directed.

Science and Technology (S&T) Liaison. A liaison from the S&T Directorate serves as the primary consultant to the PFO for all scientific and technological resource requirements to facilitate response, recovery, and mitigation. Additional responsibilities include the following:

- Represents the interests of the PFO, and provide liaison to the S&T Directorate;
- Coordinates with the Preparedness/PSD Representative deployment of detection equipment/technology (e.g., radiological pagers) and appropriate training to State and local law enforcement; and

- Provides daily input to the PFO SITREP and other reports as required or directed.

Communications/Information Technology (IT) Support Personnel. The Chief Information Officer's (CIO) liaison serves as the primary IT consultant to the PFO and is responsible for establishing all necessary linkage through technology required by the PFO to best facilitate the response effort and enable the PFO to maintain optimal situational awareness. Additional responsibilities include the following:

- Represents the interests of the PFO, and provide liaison to the Office of the CIO;
- Suggests and provides information technology solutions in order to enhance interoperability and facilitate communications by establishing management, operational, and technical controls on the IT systems supporting the incident response;
- Integrates the PFO and PFO support staff into the JFO network or virtual private network;
- Assists in the preparation of SITREPs as required;
- Assures the appropriate technology is in place to best relay SITREPs through distribution in a timely manner;
- Provides Joint Regional Information Exchange System (JRIES) (classified and unclassified) connectivity, training, and support to the PFO support staff and State and local law enforcement agencies;
- Establishes and maintains Secure Video Teleconference (SVTC) capability in support of the PFO support staff; and
- Provides and maintains cryptographic and communications security as well as classified documents handling.

PFO's Press Secretary. The DHS Public Affairs Office (PAO) will provide a representative to assist the PFO in the capacity as the overall Federal spokesperson at the incident site. Additional responsibilities include the following:

- Provides guidance and expertise to the PFO on the release of information to the media or conduct media events after consultation with the PFO;
- Upon notification, immediately coordinates with local DHS representative in the affected region and/or jurisdiction;
- Represents the interests of the PFO, and provide liaison to the DHS Public Affairs Office through the HSOC or the IIMG;
- Assists in the preparation of SITREPs and other reports as required or directed;
- Provides media, messaging, and overall communication support to the PFO and Deputy PFO on behalf of the DHS Office of Public Affairs (OPA);
- Submits to the PFO/Deputy PFO and OPA media intelligence, and a condensed report of all media stories and interactions that may affect the PFO and Deputy PFO during an incident;
- Acts as the liaison between DHS OPA and the PFO;

- Coordinates all DHS regional PAO assets and assignments as well as coordinate media logistics and locations with the affected Federal, State, and local public affairs personnel;
- Acts on behalf of and in coordination with DHS OPA and all media and communications messaging and events that will involve the PFO or Deputy PFO;
- Serves the PFO and Deputy PFO on messaging and other logistical communications needs;
- Ensures the PFO and Deputy PFO participation in the Incident Communications Emergency Plan (ICEP) and the National Incident Communications Conference Line (NICCL) conference calls;
- Coordinates response to all national media queries;
- Coordinates all Joint Information Center (JIC) assignments from affected DHS OPA components and determine other staffing assignments as needed; and
- Assists the PFO in his/her capacity as the overall Federal spokesperson for the incident.

3.1.3 Attached Liaisons

Composition of the liaison staff is based on the incident, subject-matter expertise, and/or capabilities required. The liaisons attached to the PFO support staff will perform duties associated with their parent agency or office in direct support of the PFO. Additionally, the PFO or Deputy Principal Federal Official may assign other duties or tasks in support of the mission as dictated by the incident. As the incident evolves, the liaisons attached to the PFO support staff will normally be adjusted according to the size, scope, and complexity of the incident, and will re-locate into the appropriate ESF or JFO Coordination Staff (where no appropriate ESF has been activated) once the JFO is established.

3.1.3.1 Attached DHS Liaisons

Homeland Security Operations Center (HSOC) Watch Officer. The HSOC Watch Officer is responsible to collect daily input for the PFO SITREP and assist the PFO, Deputy PFO, Chief of Staff, and the Operations Officer in developing and distributing the SITREP and other reports as required. Additional responsibilities include the following:

- Performs communications duties as directed by the PFO Deputy PFO;
- Facilitates PFO augmentation and/or reach-back from other DHS components and other Federal departments and agencies;
- Collects, logs, and tracks Requests for Information (RFIs) generated by the PFO support staff, and RFIs received from the IIMG, IMD, or DHS leadership;
- Coordinates RFIs with IAIP and other appropriate DHS staff elements;
- Coordinates RFIs with other Federal departments and agencies as appropriate;
- Briefs back answered RFIs to the PFO support staff; and
- In collaboration with the PFO support staff Communications/IT personnel, provides communications logistical support to the PFO support staff.

Preparedness Directorate/Protective Security Division (PSD) Liaison. Conducts pre-event vulnerability assessments of select high-value sites or assets in the area, if the PFO is designated in a "pre-incident" mode; supports the PFO by identifying critical infrastructure in the incident area, and the infrastructure's operational characteristics during an incident; and provides recommendations to the PFO regarding closings. Additional responsibilities include the following:

- Coordinates deployment of detection equipment/technology (e.g., radiological pagers) and appropriate training to State and local law enforcement;
- Interfaces with Federal, State and local interagency representatives on infrastructure protection issues;
- Advises the PFO on all infrastructure protection-related issues in the affected area; and
- Provides daily input to the PFO SITREP and other reports as required or directed.

DHS/FEMA Liaison. The DHS/FEMA liaison provides liaison to FEMA HQ and DHS/FEMA Regional Office/Regional Response Coordination Center (RRCC) in the affected area. Additional responsibilities include the following:

- Represents DHS/FEMA capabilities on PFO support staff;
- Ensures necessary national and regional assets are available to the PFO, if required; and
- Provides daily input to the PFO SITREP and other reports as required or directed.

Customs and Border Protection/Immigration and Customs Enforcement/Transportation Security Administration Liaisons

- Provides liaison to each agency's Headquarters components;
- Represents each agency's respective capabilities on PFO support staff;
- Coordinates with regionally based Customs and Border Protection (CBP), Federal Air Marshals Service (FAMS), Transportation Security Administration (TSA), Federal Protective Service (FPS) and Immigration and Customs Enforcement (ICE) offices to ensure necessary assets are available to the PFO; and
- Provides daily input to the PFO SITREP and other reports as required or directed on the status of rail, air, and maritime security.

Office of State and Local Government Coordination and Preparedness (OSLGCP) Liaison. TheOSLGCP will provide a representative to assist the PFO in his/her interactions with the State and local government officials in order to facilitate the response effort. Additional responsibilities include the following:

- Represents the interests of the PFO, and provide liaison to the OSLGCP through the HSOC or the IIMG;
- Upon notification of an incident, immediately coordinates with local DHS representative in the affected jurisdiction;

- Establishes liaison with the state, local and tribal government officials in order to share information and enhance situational awareness for the PFO; and
- Provides daily input to PFO SITREPs and other reports as required or directed.

Private Sector Office Liaison

Primary responsibilities include the following:

- Provides liaison with the Office of Private Sector Liaison;
- In collaboration with the Preparedness Directorate/PSD PFO support staff member, coordinates with private-sector representatives in the affected area/sectors;
- Provides guidance and expertise to the PFO on issues related to private sector; and
- Provides daily input to the PFO SITREP and other reports as required or directed.

United States Coast Guard (USCG) Liaison

Primary responsibilities include the following:

- Provides liaison to USCG headquarters and local offices;
- Represents USCG capabilities on the PFO support staff;
- Ensures necessary USCG assets are available to the PFO, if required;
- Assists PFO by providing on-scene consultation and reach-back capability regarding maritime safety, security and response; and
- Provides daily input to the PFO SITREP and other reports as required or directed.

United States Secret Service (USSS) Liaison

Primary responsibilities include the following:

- Provides liaison to DHS/USSS headquarters and local offices;
- Represents DHS/USSS capabilities on the PFO support staff;
- Ensures necessary DHS/USSS assets are available to the PFO, if required;
- Assists PFO by providing on-scene consultation and reach-back capability regarding maritime security and response; and
- Provides daily input to the PFO SITREP and other reports as required or directed.

3.1.3.2 Attached Interagency Liaisons

Federal Bureau of Investigation (FBI) Liaison Officer. The FBI liaison officer maintains the liaison between FBI Headquarters, the FBI local office, the JOC, the SIOC, and the PFO support staff. Additional responsibilities include the following:

- Provides subject-matter expertise;
- Provides reach-back capability; and
- Provides daily input to the PFO SITREP and other reports as required or directed.

Department of Health and Human Services (HHS) Liaison. The HHS liaison officer assists the PFO by providing on-scene consultation and reach-back capability regarding health and medical services issues, and epidemiological support/guidance on the medical implications in case of mass casualty incidents. Additional responsibilities include the following:

- Provides the following types of information to the PFO and cell members on a daily basis (pending availability of this information from the health agency with appropriate jurisdiction):
  - Any available clinical surveillance results for last 24-hour period, including significant illness or disease information;
  - Number and type of cases seen at venue and any National Disaster Medical System (NDMS) medical station(s), with additional information about any subsequent transports out of the secure zone, if available;
  - Hospital bed and blood availability (with comparison to baseline numbers for this period);
  - Results, if available, of any environmental monitoring of venue; and
  - Any other "going forward" health/medical concerns for the next coordination period (including, for example, other large events that may have health/medical impact);
- Interacts regularly with S&T, Office of Intelligence & Analysis and Preparedness Directorate staff members to ensure mutual, reciprocal connectivity on all public health/medical matters; and
- Prepares, in concert with HHS Secretary's Emergency Response Team (SERT) team leader, daily input to the PFO SITREP and other reports as required or directed.

3.1.4 Other Attached Staff

As outlined in Section 3.3.3.1 of the SOP, the JFO Coordination Staff will provide safety, legal counsel, equal rights, and security advice to the PFO and JFO Coordination Group once established within the JFO. During the initial stages of incident management, however, this staff may not yet be established. Accordingly, the PFO may request additional staff be attached to the PFO support staff from other DHS or non-DHS entities based on the incident in order to provide expertise or augment personnel requirements, for example, requesting general counsel from the strategic legal section to address specific issues at a meeting or press conference, or an HHS representative in a plague scenario. The preference of the PFO, based on the assessment of the incident, will dictate how the staff is configured. As with the liaison staff, these other attached staff will move to the JFO Coordination Staff once the JFO is established.

3.1.5 PFO's Advance and Security Elements

The PFO will require an advance team to coordinate movements and logistics, maintain schedules, maintain liaison with the PFO support staff and JFO Coordination Staff when the PFO is traveling, etc. In the event a security element is required, both the PFO advance and security elements will be scaled accordingly to meet mission requirements.

3.2 PFO Support Staff Role in the JFO

The PFO support staff will be organized in accordance with the NIMS. This organization is intended to support each of the four sections that could operate under the NIMS structure: Operations, Planning, Logistics, and Finance and Administration.

3.2.1 Support to the JFO Operations Section

The PFO, in concert with the JFO Coordination Group, synchronizes the incident management operation. The PFO support staff ensures effective management of the PFO's priorities while maintaining focus on strategic and policy issues.

3.2.2 Support to the JFO Planning Section

The PFO support staff, in concert with the JFO, IIMG, and the HSOC, provides current information to the PFO in order to: ensure situational awareness, determine cascading effects of the incident area, identify national implications, and determine specific areas of interest requiring long-term attention.

3.2.3 Support to the JFO Logistics Section

Once the PFO support staff receives an activation and/or deployment order, they will coordinate administrative and logistical support required under ESF #5 for deployment and sustainment of the PFO and staff with the appropriate agency.

3.2.4 Support to the JFO Finance and Administration Section

The PFO support staff monitors all funding requirements under ESF #5 in order to ensure that the PFO maintains awareness of all costs relating to the incident.

3.3 PFO Relationships

The PFO will monitor the deployment and application of Federal assets and resources through the unified command concept in support of the designated incident commander, in collaboration with other Federal officials identified in existing plans, such as the FCO and the FBI SAC. The FCO, the FBI SAC, and other Federal incident management officials designated in existing plans will maintain their basic authorities and responsibilities as defined in the NRP and other existing plans, statutes, and Presidential directives. Nothing in this document alters or impedes the ability of Federal, State, local, or tribal departments and agencies to carry out their specific authorities or perform their responsibilities under all applicable laws, Executive orders, and directives.

3.3.1 To the Interagency Incident Management Group (IIMG)

The IIMG is a Federal headquarters-level multiagency coordination entity that facilitates strategic Federal domestic incident management for Incidents of National Significance. The Secretary of Homeland Security activates the IIMG based on the nature, severity, magnitude, and complexity of the threat or incident. Its membership is tailored and scaled to address the specific event. The IIMG provides strategic guidance to the Secretary of Homeland Security and maintains ongoing coordination with the PFO and JFO Coordination Group. The IIMG Director will receive information directly from the PFO, DHS liaison officers, or non-DHS officials as needed. The PFO will provide input

to the IIMG Director for situation reports and other updates for the Secretary and other members of the senior DHS leadership as required. The PFO will assist the IIMG in recommending courses of action and framing decisions for the senior leadership. The IIMG is activated upon recall from the Secretary or his/her designated representative in the event of an incident. The IIMG will provide the designated PFO with information in order to provide the best possible situational awareness. For additional information on IIMG activities, see the IIMG SOP (published separately).

3.3.2 To the Office of Operations Incident Management Division

The IMD will serve as the conduit for steady-state communications from the Secretary or DHS Headquarters to the PFO Network. The PFO Network is the cadre of trained personnel throughout the United States who may serve in the capacity of Principal Federal Official. To ensure that the PFO Network has proper support for resources, training, exercises, and operations, the IMD will designate representatives to serve as PFO Coordinators. The IMD PFO Coordinators will be responsible for:

- Drafting appropriate correspondence from the Secretary regarding the PFO network;
- Drafting PFO designation documents for Incidents of National Significance, National Special Security Events (NSSE), and training/exercise events;
- Developing training/exercise schedules and related materials for the PFO Network;
- Conducting a needs assessment and subsequent training and exercises for the PFO Network;
- Developing and maintaining a current contact list for the PFO Network;
- Serving as the PFO Network's steady-state liaison to the Secretary and the HSOC;
- Conducting regular conference calls and/or video teleconferences (VTCs) with the PFO Network to share information and provide updates on policies that may impact potential PFOs;
- Upon Secretarial designation of a PFO, serving as the overall coordinator in conjunction with ESF-5 for the PFO's initial transportation and communication package;
- In consultation with the designated PFO, determining the composition of a PFO support staff, notifying the supporting DHS component, and assisting with the deployment of that component's PFO support staff designee;
- Notifying the NRCC of resource requirements;
- Deploying with the PFO support staff to serve as Operations Officer and IMD representative;
- Providing program support and policy guidance for the PFO/PFO support staff.

3.3.3 To the Homeland Security Operations Center and National Response Coordination Center

The HSOC is the primary national hub for domestic incident management, operational coordination, and situational awareness. The PFO will establish incident reporting requirements in concert with the HSOC to ensure appropriate information is available to the Secretary and the IIMG. For additional information on HSOC activities, see the HSOC SOP (published separately).

The HSOC/NRCC is a multiagency center that provides overall Federal response coordination for incidents of National Significance and emergency management program implementation. The HSOC/NRCC is a functional component of the HSOC in support of incident management operations. For additional information on HSOC/NRCC activities, see the NRCC SOP (published separately).

3.3.4 To the JFO Coordination Group

[RESERVED].

4.0 Logistical Requirements

The logistical support package will be addressed in the following areas: Transportation, Communications/IT, and Administrative.

4.1 Transportation

The PFO support staff must be able to deploy to any incident location immediately upon notification in accordance with recall and deployment procedures (TBD). During the PFO's initial assessment of the incident, he/she will determine a primary and alternate means of deployment to the affected jurisdiction. The Deputy PFO in conjunction with the IIMG will arrange the most expedient deployment option available from the following options:

- Internal DHS fixed-wing assets (USCG/CBP-AMO)
- DOD aircraft
- Leased aircraft
- Commercial airlines
- Ground transportation
- Watercraft

Upon arrival in the affected jurisdiction, the PFO and Staff will require sufficient ground transportation and off-loading equipment to deploy the staff and equipment to the incident command post and provide mobility within the affected jurisdiction.

4.2 Communications

The PFO support staff must have the ability to establish and maintain effective and timely communications, in order to manage the incident. The following equipment is required by the PFO support staff and is to be made available in a "go-kit" to accomplish this task:

QUANTITY	ITEM
2	Pelican Cases
10	Cellular Phones with secure capability
2	STU/STE Phones
1	Secure Fax
1	Secure Video Teleconference
12	Laptop Computers
1	16 port 10/100 switch

20	USB Portable Drives (512mb min.)
2	Portable Computer Printers w/4800 dpi Color
12	Sets extra peripherals for all electronic equipment (Chargers, cables, cords, power strips, networking hardware, etc.)
1	Set Office Supplies (should include) • Pens and Pencils • Whiteboard Markers • Scissors • Paper Pads • Stenographer Pads • Printer/Copier Paper • Stapler and Staples • Three and Two Hole Punches • Tape (All types) • Highlighters • Printer Cartridges • File Folders • Document Protectors • Blank Floppy Disks • Blank CD-RWs • Cardboard File Boxes • Paper and Binder Clips

4.3 Administrative Requirements

The PFO support staff must have internal administrative support in order to sustain itself independently in the initial deployment and establishment of the command post at the incident site. The following list of basic administrative supplies is adequate to adjust to various locations and scenarios:

QUANTITY	ITEM
10	Folding Tables (6'x3')
20	Folding Chairs
2	Portable Folding Easels with Whiteboard
1	Cross-cut Paper Shredder
3	Televisions with VCR capability
3	TV Stands

5.0 Administration and Logistics

Administrative reports and record keeping are outlined in Tabs 2 through 9 to this Annex.

Tab 1 to Annex G: Warning Order Format

In certain scenarios, a PFO may be pre-designated by the Secretary of Homeland Security to facilitate Federal domestic incident planning and coordination at the local level outside the context of a specific threat or incident. A PFO may also be designated in a pre-incident mode for a specific geographic area based on threat and other considerations. The warning order below outlines the basic information transmitted in these circumstances to the pre-designated PFO and support staff.

1.0 Situation

1.1 Incident Situation

1.1.1 Incident

1.1.2 Status of Infrastructure (roads, power, water—provide maps)

1.2 Agencies Involved

1.2.1 ERT and JOC Personnel

1.2.2 Other Response Forces (Federal, State, and local)

1.2.3 Civil Organizations (Federal, State, and local)

1.2.4 Private Sector and Tribes

2.0 Mission (Who, What, When, Where, and Why)

3.0 Execution (Information from OPORD)

Secretary's Intent (purpose, method, end-state)
PFO's Intent (purpose, method, end-state)

3.1 Concept of Operations

3.2 Tasks for sections

3.3 Tasks for individuals

3.4 Coordinating Instructions

3.4.1 Timeline

3.4.2 PFO Requirements

3.4.3 SITREP

3.5 Future Plans (redeployment)

3.5.1 Projected date

3.5.2 Phased or total unit

4.0 Logistic Support (See Annex D)

4.1 Support Concept (GSA/local government/agency sources)

4.2 Materiel and Services (lodging/dining/fuel/supplies, maintenance, etc.)

4.3 Medical evacuation and hospitalization (locations of support/procedures)

4.4 Personnel Support (mail, religious support, MWR, safety, awards, etc.)

5.0 Communications

- 5.1 Operations Centers (JFO, JOC, local EOC, and civil authorities/locations)
- 5.2 Means of Communications
- 5.3 Phone Directory

Tab 1 to Annex G: Reports/Scheduled Events

REPORTS/SCHEDULED EVENTS (Battle Rhythm)

TIME	DATE OR FREQUENCY	REPORT/EVENT	RESPONSIBLE	CODE	DATE/COMPLETED OR REMARK

STATUS: C-Completed (Reports-put date in remarks), A-Attended Meeting, L-Logged (Information in Daily Staff Journal)

Tab 2 to Annex G: Mission Points of Contact

MISSION POINTS OF CONTACT

ORGANIZATION	NAME	PHONE	CELL	BEEPER	FAX	E-MAIL

Tab 3 to Annex G: Weather

Tab 4 to Annex G: Request for Information

1.0 Action Tracking Log Templates

Action Tracking Log

DTG	Action Number	Priority (High, Med, or Low	Requested Action	Assigned To	Requested By	Action Receipt DTG	Suspense DTG	Completion DTG	Contact Information

Tab 5 to Annex G: Communications Tracking Log

Communications Tracking Log

DTG	Call #	From	To	Subject	Associated Taskers	Tasker Priority	Suspense DTG	Completion DTG

Tab 6 to Annex G: Attendance Tracking Log

Department/Agency	Name (Last, First)	In/Out & Location	Arrival Time	Location	Contact Information

Tab 7 to Annex G: Requests for Information Tracking Log

Request for Information Tracking Log

DTG	Action Number	Priority (High, Med, or Low	Requested Action	Assigned	Requested By	Action Receipt DTG	Suspense DTG	Completion DTG	Contact Information

Tab 8 to Annex G: Financial Information

FINANCIAL INFORMATION

MA NUMBER	MISSION	AMOUNT ALLOCATED	AMOUNT PER DAY	START DATE/TIME	CURRENT DATE/TIME	AMOUNT TO DATE	DATE 5A RMO NOTIFIED	ADDTL $s REQ. (Y/N)	DATE ADDTL $s REQUESTED	ALLOCATED ALL MISSIONS

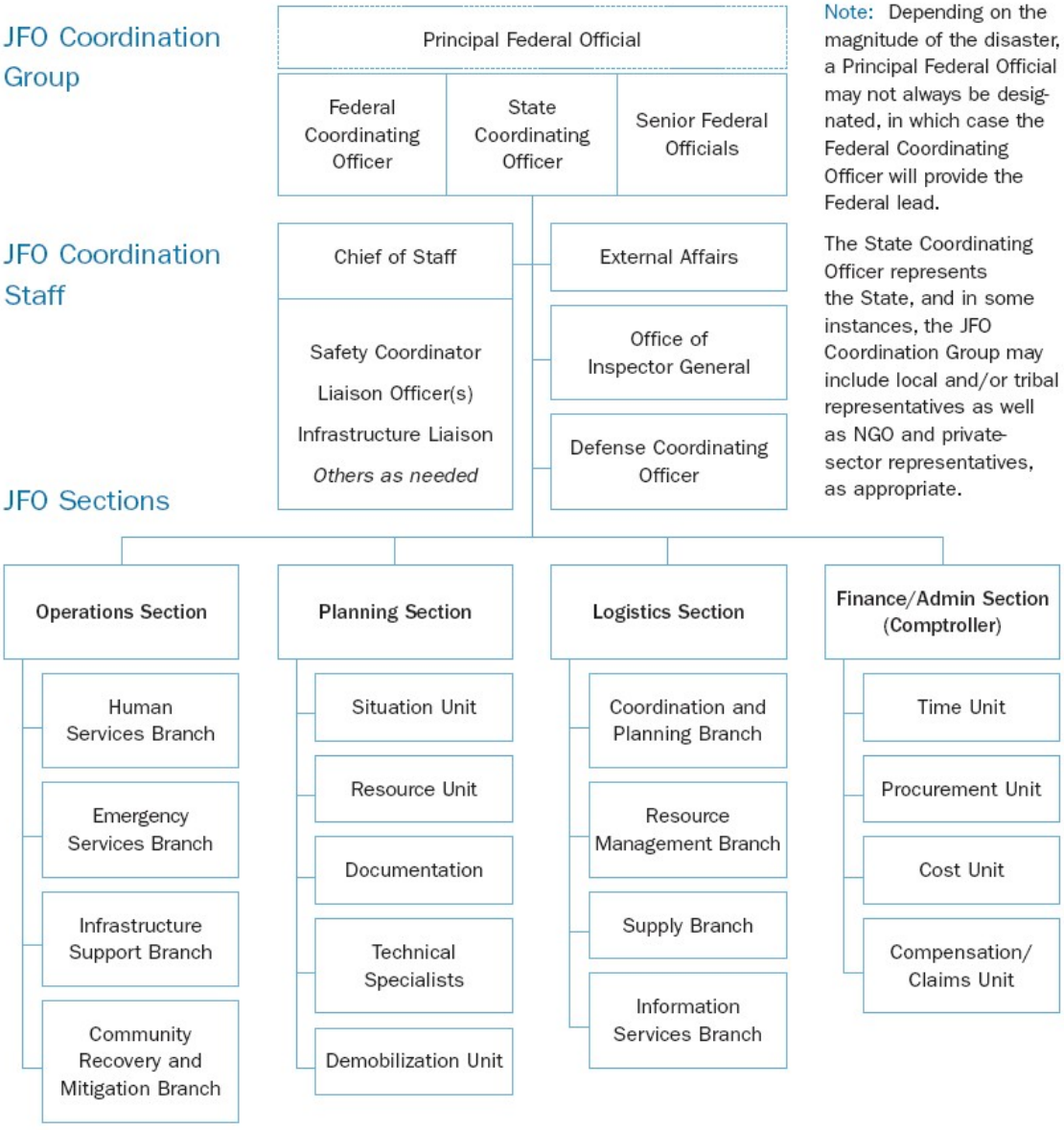
Tab 9 to Annex G: Domestic Emergency Support Team (DEST)

[RESERVED]

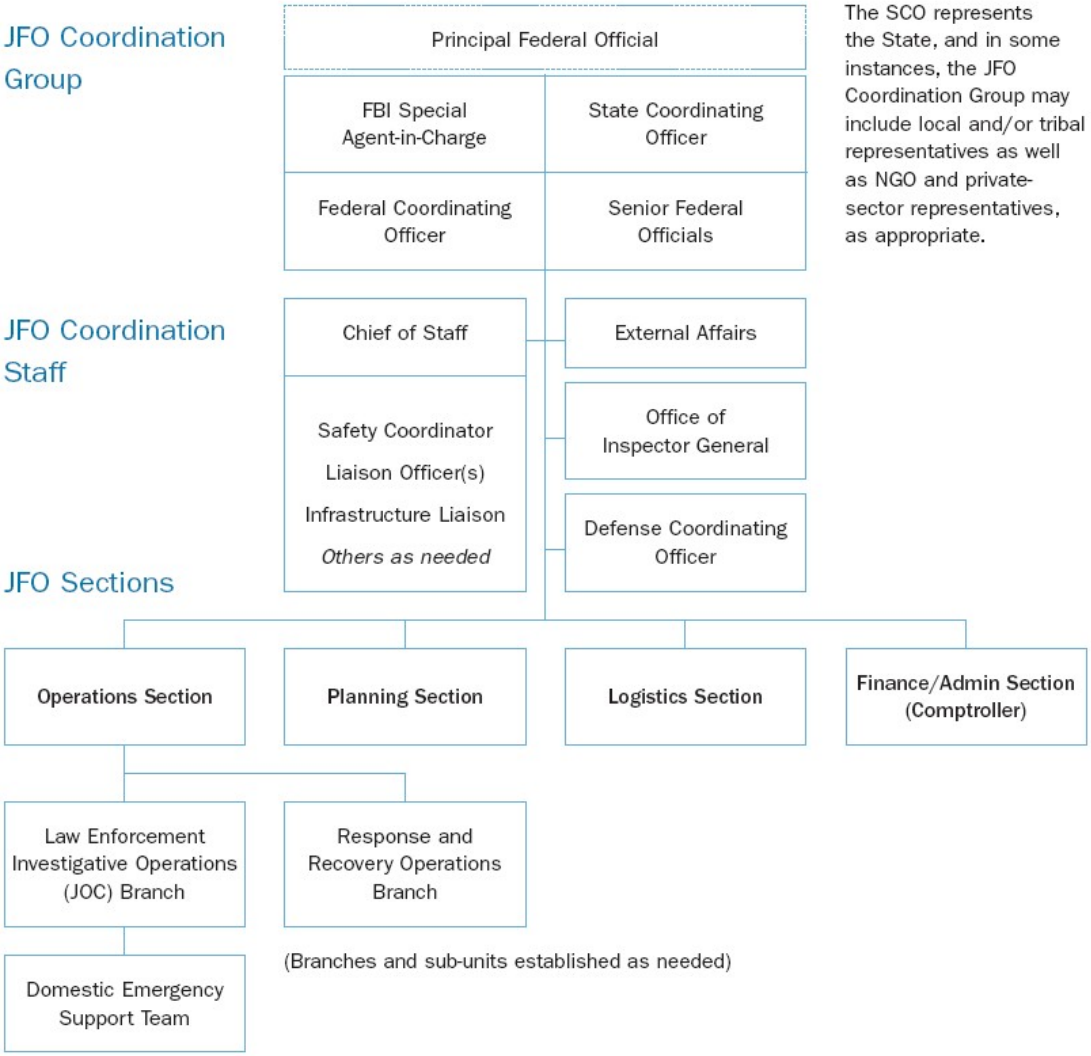
Annex H: Joint Field Office Organization

Figures 1 through 4 illustrate possible JFO organizational structures for various types of threat scenarios and incidents. Figure 1 illustrates the organization for natural disasters, Figure 2 shows modifications for terrorism, Figure 3 shows modifications for incidents involving Federal-to-Federal support, and Figure 4 depicts the JFO organization for a National Special Security Event (NSSE). All or portions of these organizational structures may be utilized based on the nature and magnitude of the threat or incident.

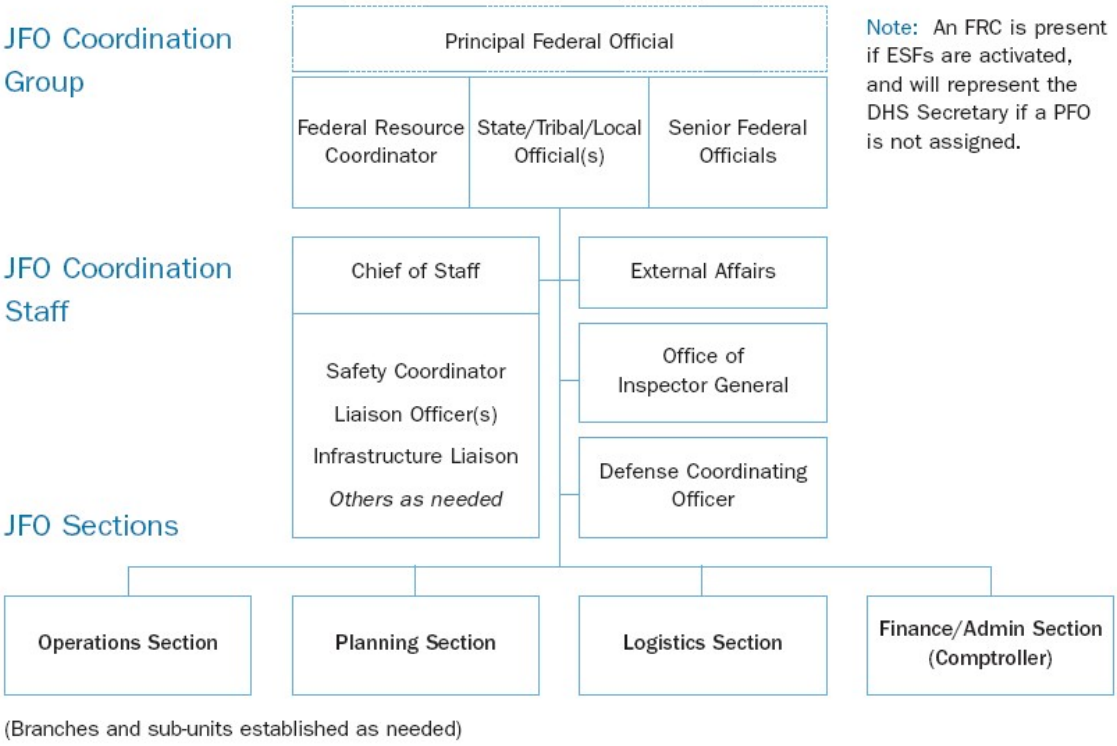
Tab 1 to Annex H: Sample JFO Organization for Natural Disasters



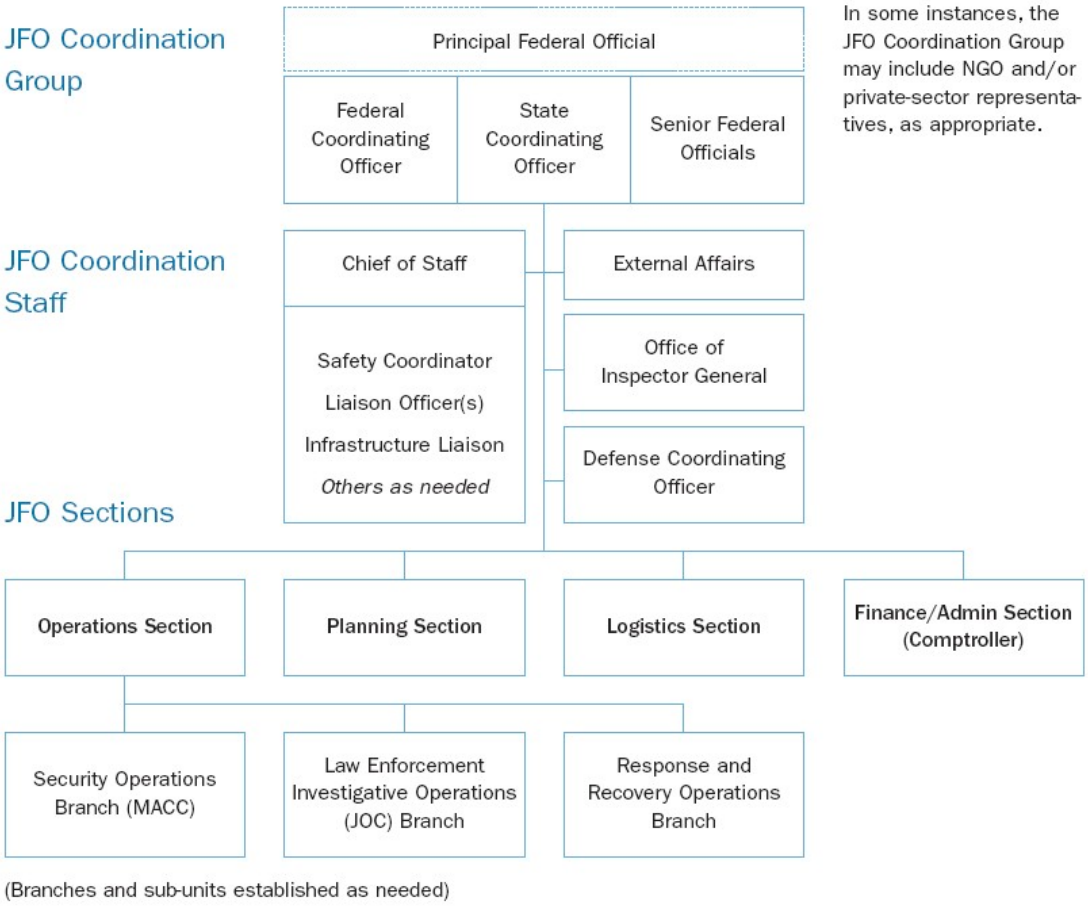
Tab 2 to Annex H: Sample JFO Organization for Terrorism Incidents



Tab 3 to Annex H: Sample JFO Organization for Federal-to-Federal Support



Tab 4 to Annex H: Sample JFO Organization for National Special Security Events



Annex I: Joint Information Center

[RESERVED]

Annex J: JFO Exercise Evaluation Guidelines

Task# JFO-1: Alert and Mobilize JFO Staff	
Outcome: Emergency Management	Location: JFO
Response Element: JFO Staff	Jurisdiction:
Evaluator:	Contact #:

Follow-up Analysis	
Upon completion of the day's exercise play, evaluators should compile their observations into a chronological narrative of events, describing outcomes achieved or not achieved. For any outcomes that are not achieved, the evaluator should analyze the sequence of events and attempt to determine the cause using the questions at right. The questions below may further help determine root cause.	• What happened? • What was supposed to happen? • If there is a difference, why? • What is the impact of that difference? • What should be learned from this? • What corrective actions are recommended?

1. Were the PFO/FCO/FRC or designated alternate notified of the incident in a timely manner?
   a. How was this notification made?
   b. How long did it take?
2. Did the appropriate authority authorize activation of the JFO? Who authorized the activation (name and title)?
3. Did HSOC initiate alert/recall procedures for JFO personnel? Was the recall list current? Did "on-duty" personnel or substitutes respond?
4. Was the JFO accessible to the agencies or participants represented? Where was it located?
5. Was the JFO established in a safe and secure area? What security measures were used?
6. Did the appropriate staff respond to the recall?
7. Did the JFO effectively integrate the JOC, PFO support staff, MACC, and JIC, as appropriate?

Task# JFO-2: Activate, Expand, and Operate the JFO	
Outcome: Emergency Management	Location: JFO
Response Element: JFO Staff	Jurisdiction:
Evaluator:	Contact #:

Follow-up Analysis	
Upon completion of the day's exercise play, evaluators should compile their observations into a chronological narrative of events, describing outcomes achieved or not achieved. For any outcomes that are not achieved, the evaluator should analyze the sequence of events and attempt to determine the cause using the questions at right. The questions below may further help determine root cause.	• What happened? • What was supposed to happen? • If there is a difference, why? • What is the impact of that difference? • What should be learned from this? • What corrective actions are recommended?

Activation/Notification

1. Was the incident declared a disaster under the Stafford Act and/or an Incident of National Significance?
2. Was the appropriate JFO level established in response to the incident?
3. Did the appropriate authority authorize activation of the JFO? Who authorized the activation (name and title)?
4. Was the JFO established in a manner to allow a scalable expansion as the incident developed?
5. What procedures were established to maintain a communications link or liaison with the incident scene, the State EOC, and other Federal commands, if not collocated in the JFO?
6. Were the participants you observed stopped, identified, and badged prior to entering the JFO? How was this conducted?
7. Were all agencies advised of the JFO's location? What agencies were notified? How were they notified?
8. Was the activation and response coordinated and efficient?
9. How effective was the HSOC/DHS "Communicator" system? Were there any problems with the notification procedures? If so, please describe.
10. Were arriving staff appropriately briefed upon their arrival?

Roles and Responsibilities

11. Did the FCO/FRC or designated alternate assume overall control of JFO operations?
12. What was the name and title of the person assuming control?
13. Describe the overall level of control maintained in the JFO – did the FRC/FCO maintain appropriate control?
14. Describe the FCO/FRC's use of available resources and staff positions – were they appropriately used to maximize efficiency and effective response operations? Were staff sufficiently trained to accomplish their duties?
15. Did the appropriate PFO/FCO/FRC/SFLEO/MACC SFLEO understand their relationships to each other? Did they understand the roles of the JFO staff?
16. Did the FCO/FRC have authority to use necessary resources to mitigate the emergency and coordinate additional elements?
17. What liaisons from participating agencies/departments were present at the JFO?
18. Were the agencies/departments you observed properly equipped to perform their functions? Please list any missing equipment/communication devices, etc.
19. Describe the organization of the JFO (sections/branches)?
20. How were the ESFs distributed among the sections/branches?

JFO Sections

21. Was the Operations Section divided into the following, as appropriate to the incident?
    a. Law Enforcement Investigative Branch (JOC)?
    b. Response & Recovery Branch?

c. Security Operations Branch (MACC)?

22. Was the Planning Section successful at providing situational awareness, identifying national implications, anticipating cascading effects, and determining the status of Federal resources?
    a. Was the HSOC/IIMG kept properly informed?
    b. Were requests for technical and scientific expertise coordinated by the Planning Section?
    c. Did the Planning Section successfully integrate the intelligence function?
23. Was the Logistics Section effective in supplying support to the JFO and to incident personnel (upon request)?
    a. Were the appropriate units established (Supply, Facilities, Ground Support, Air Operations Support, Communications, Medical)?
24. Was the Finance/Administration Section effective at managing, monitoring, and tracking all Federal costs associated with the JFO?
    a. Did the Comptroller effectively act as a Senior Financial Advisor to the JFO Coordination Group and the Chief Financial Officer of the controlling agency? Did the JFO Coordination Group receive timely updates on financial expenditures relating to the incident?
    b. Was the Finance/Administration Section organized with the appropriate units (Time/Procurement/Compensation & Claims, Cost)?

Task# JFO-3: JFO Operations	
Outcome: Emergency Management	Location: JFO
Response Element: JFO Staff	Jurisdiction:
Evaluator:	Contact #:

Follow-up Analysis	
Upon completion of the day's exercise play, evaluators should compile their observations into a chronological narrative of events, describing outcomes achieved or not achieved. For any outcomes that are not achieved, the evaluator should analyze the sequence of events and attempt to determine the cause using the questions at right. The questions below may further help determine root cause.	• What happened? • What was supposed to happen? • If there is a difference, why? • What is the impact of that difference? • What should be learned from this? • What corrective actions are recommended?

Operations

1. Were JFO operations consistent with plans, procedures, and protocols? Were plans sufficient for response to the range of incident scenarios?
2. Describe the FRC/FCO's understanding of their authority to use necessary resources to mitigate the emergency and coordinate additional elements.
3. Did the JFO, in consultation with State and local counterparts, analyze information/data to formulate mitigation and forward-looking corrective actions? Describe how.
4. Did JFO personnel maintain an account/log of incident events? How was this done?
5. Was there a smooth rotation of personnel for each shift change? How was this maintained?
6. Were situation reports given to all agencies when necessary? How often and by whom?
7. Was a determination of incident stabilization and termination of command made? How and by whom?

Coordination

8. Was the response to the incident unified and integrated? Did the agencies involved demonstrate good teamwork and coordination? Describe.
9. Were there written agreements in place between appropriate agencies? If not, did the lack of agreements have an effect on coordination?
10. Were MOUs/MOAs implemented?
11. Was information/data coordinated and communicated among coordination elements?
12. Based on your observations, would you say communication with other sections was adequate? On site, face to face? On site, radio? On site, agency to agency?

Task# JFO-4: Coordinate with Government Agencies and Officials	
Outcome: Emergency Management	Location: JFO
Response Element: JFO Staff	Jurisdiction:
Evaluator:	Contact #:

Follow-up Analysis	
Upon completion of the day's exercise play, evaluators should compile their observations into a chronological narrative of events, describing outcomes achieved or not achieved. For any outcomes that are not achieved, the evaluator should analyze the sequence of events and attempt to determine the cause using the questions at right. The questions below may further help determine root cause.	• What happened? • What was supposed to happen? • If there is a difference, why? • What is the impact of that difference? • What should be learned from this? • What corrective actions are recommended?

1. Describe the process for notification to local, State, tribal, and other Federal entities.
2. Was there a coordinated response in sharing information with local, State, and Federal agencies and officials?
3. Were any key components overlooked?
4. Were the roles and functions of each level of government recognized, understood, and adequately performed?
5. Were all potentially impacted jurisdictions considered and included in coordination?
6. Was a PFO designated to coordinate among agencies?

Task# JFO-5: Coordinate Public Information Activities	
Outcome: Emergency Management	Location: JFO
Response Element: JFO Staff (Public Affairs)	Jurisdiction:
Evaluator:	Contact #:

Follow-up Analysis	
Upon completion of the day's exercise play, evaluators should compile their observations into a chronological narrative of events, describing outcomes achieved or not achieved. For any outcomes that are not achieved, the evaluator should analyze the sequence of events and attempt to determine the cause using the questions at right. The questions below may further help determine root cause.	• What happened? • What was supposed to happen? • If there is a difference, why? • What is the impact of that difference? • What should be learned from this? • What corrective actions are recommended?

Communications Plan

1. Was a single media point of contact established early in the incident? Who and where?
2. Was a media conference area established? Was the need for regular briefings and information releases recognized and acted upon? Who provided the briefings?
3. How did the agencies involved prepare and coordinate news releases for dissemination and/or conduct press conferences for the local media?
4. What actions were taken within the JFO to handle public inquiries?
5. If an Incident of National Significance, did a DHS PAO assume the position of PFO's Press Secretary?
6. What procedures were used to ensure essential incident information was provided to the PFO's Press Secretary?
7. How was the media plan developed? Was it implemented in an effective and timely manner?

Dissemination of Public Information

8. What procedures were used to publicly disseminate information?
9. What information was provided to the public to educate them about potential hazards and risk reduction methods?
10. How did the media plan use media outlets to keep the public informed?
11. Was there any use of the Emergency Broadcast System?

Agency Coordination Protocols

12. Were situation reports given to all agencies where necessary? How often and by whom?
13. How was critical/sensitive information disseminated to the Secretary, HSOC, and IIMG (e.g., by VTC, by telephone, by fax)?
14. What measures were taken to coordinate with the Governor's press secretary on a recurring basis?
15. How was coordination established with Federal and State agencies before their inclusion in the JIC?
16. What measures were taken to ensure a common government message?
17. Was a JIC established? Why or why not?

Task# JFO-6: Activate and Operate JIC	
Outcome: Emergency Management	Location: JIC
Response Element: JIC	Jurisdiction:
Evaluator:	Contact #:

Follow-up Analysis	
Upon completion of the day's exercise play, evaluators should compile their observations into a chronological narrative of events, describing outcomes achieved or not achieved. For any outcomes that are not achieved, the evaluator should analyze the sequence of events and attempt to determine the cause using the questions at right. The questions below may further help determine root cause.	• What happened? • What was supposed to happen? • If there is a difference, why? • What is the impact of that difference? • What should be learned from this? • What corrective actions are recommended?

JIC Activation

1. Did public information staff report to the JFO or JIC in a timely manner?
2. What agencies and organizations were represented in the JIC?
3. Were any agencies missing that should have been included in the JIC? Who and why?
4. What procedures were followed to establish a JIC?

JIC Operation

5. How was the location of the JIC determined? How was information disseminated to agencies and the media?
6. Was the JIC organized to effectively execute its role? Were supporting agencies adequately staffed and equipped to perform their functions in the JIC?
7. What plans have been developed to support a JIC expansion to accommodate State and local involvement?
8. What actions were taken to set criteria for and control of access to the JIC?
9. How was coordination established with Federal and State agencies before their inclusion in the JIC?
10. What was the procedure for the approval of press releases? Who had final approval authority?
11. Were public messages correct and consistent among JIC staff and remote public information staff?
12. How were messages from various entities deconflicted?

JIC Staffing and Equipment

13. What volume of calls (media and public) did the JIC have to manage?
14. How adequate was the staffing in relation to the call volume and need to prepare press releases and briefings?
15. How adequate was the equipment provided (computers, fax, copiers, telephones, etc.) to manage the volume of public and media inquiries?

Task# JFO-7: Provide Emergency Public Information	
Outcome: Emergency Management	Location: JIC
Response Element: PIO/JIC	Jurisdiction:
Evaluator:	Contact #:

Follow-up Analysis	
Upon completion of the day's exercise play, evaluators should compile their observations into a chronological narrative of events, describing outcomes achieved or not achieved. For any outcomes that are not achieved, the evaluator should analyze the sequence of events and attempt to determine the cause using the questions at right. The questions below may further help determine root cause.	• What happened? • What was supposed to happen? • If there is a difference, why? • What is the impact of that difference? • What should be learned from this? • What corrective actions are recommended?

Information Gathering and Analysis

1. How did the public information staff gather and share essential incident information?
2. How did the public information staff gather information from the public and media to ensure that their message was being properly received?
3. What trends in media reporting were identified and provided to the PFO's Press Secretary and emergency management officials?
4. What trends in public inquiries and rumors were identified and provided to the PFO's Press Secretary and emergency management officials?

Dissemination of Public Information

5. What procedures were used to publicly disseminate information?
6. How frequently were press releases issued?
7. What procedures were used for press release approval?
8. What information was provided to the public to educate them about potential hazards and risk reduction methods?
9. How was this information checked with technical experts to ensure it was accurate before release?
10. How was use of the Emergency Broadcast System coordinated to disseminate information to the public?
11. How did the media plan use media outlets to keep the public informed?

Agency Coordination Protocols

12. Were situation reports given to all agencies where necessary? How often and by whom?
13. How was critical/sensitive information disseminated to agencies (e.g., in person, by telephone, by radio)?
14. What measures were taken to coordinate with the Governor's press secretary on a recurring basis?
15. How was coordination established with Federal and State agencies before their inclusion in the JIC?
16. What measures were taken to ensure a common government message?
17. Was a JIC established? Why or why not?

Task# JFO-8: Emergency Support Functions (ESFs)	
Outcome: Emergency Management	Location: JFO
Response Element: JFO Coordination Group	Jurisdiction:
Evaluator:	Contact #:

Follow-up Analysis	
Upon completion of the day's exercise play, evaluators should compile their observations into a chronological narrative of events, describing outcomes achieved or not achieved. For any outcomes that are not achieved, the evaluator should analyze the sequence of events and attempt to determine the cause using the questions at right. The questions below may further help determine root cause.	• What happened? • What was supposed to happen? • If there is a difference, why? • What is the impact of that difference? • What should be learned from this? • What corrective actions are recommended?

1. Did the JFO use a structured approach to the activation of ESFs?
2. Was ESF support tailored to the type, extent, and duration of the event or situation?
3. Did the appropriate Primary/Support Agency(s) participate in the ESF functions?
4. Did Federal agencies with independent authority continue to perform their agency statutory responsibilities outside the ESF?
5. How were the ESFs organized within the ICS structure?

Task# JFO-9: JFO Coordination Group	
Outcome: Emergency Management	Location: JFO
Response Element: JFO Coordination Group	Jurisdiction:
Evaluator:	Contact #:

Follow-up Analysis	
Upon completion of the day's exercise play, evaluators should compile their observations into a chronological narrative of events, describing outcomes achieved or not achieved. For any outcomes that are not achieved, the evaluator should analyze the sequence of events and attempt to determine the cause using the questions at right. The questions below may further help determine root cause.	• What happened? • What was supposed to happen? • If there is a difference, why? • What is the impact of that difference? • What should be learned from this? • What corrective actions are recommended?

1. Did the appropriate authority authorize activation of the JFO? Who authorized the activation (name and title)?
2. Was the JFO Coordination Group appropriately sized for the incident?
3. Was the JFO established in a manner to allow a scalable expansion as the incident developed?
4. Did the appropriate PFO/FCO/SFLEO understand their relationships to each other?
5. Was the JFO staffed with appropriate level personnel from the appropriate agencies? Was this accomplished smoothly?
6. Was a PFO designated for this event? How was the PFO support staff incorporated into the JFO?
7. Was the appropriate PFO support staff integrated into the JFO staff/sections as the incident progressed?

Task# JFO-10: Emergency Response and Support Teams	
Outcome: Emergency Management	Location: JFO
Response Element: JFO Operations Section	Jurisdiction:
Evaluator:	Contact #:

Follow-up Analysis	
Upon completion of the day's exercise play, evaluators should compile their observations into a chronological narrative of events, describing outcomes achieved or not achieved. For any outcomes that are not achieved, the evaluator should analyze the sequence of events and attempt to determine the cause using the questions at right. The questions below may further help determine root cause.	• What happened? • What was supposed to happen? • If there is a difference, why? • What is the impact of that difference? • What should be learned from this? • What corrective actions are recommended?

1. Was the ERT requested by the JFO Coordination Group?
   a. Was the request properly routed from the JFO Coordination Group to the RRCC?
   b. Was there a timely request for ERT support? Was the ERT response to the JFO timely?
   c. Who in the JFO Coordination Group authorized the request for the ERT?
   d. Did ERT personnel properly staff the sections and branches after initial reporting/set-up responsibilities were satisfied in the JFO?
   e. How was the ERT transported? Were there any delays/problems with deployment?
2. Did the situation/incident warrant deployment of the National Emergency Response Team (ERT-N)? If so:
   a. Was the ERT-N deployment coordinated through the National Response Coordination Center (NRCC)?
   b. Did the DHS Under Secretary for Preparedness authorize deployment?
   c. Was the on-call team utilized? If not, why not?
   d. Did the ERT-N personnel properly staff the sections and branches after initial reporting/set-up responsibilities were satisfied in the JFO?
   e. How was the ERT-N transported? Were there any delays/problems with deployment?
3. Did the situation/incident warrant deployment of the Domestic Emergency Support Team (DEST)? If so:
   a. Did the local FBI SAC make the request?
   b. Was the request coordinated through the Director, FBI and the DHS Under Secretary for Preparedness?
   c. Were the AG and DHS Secretary consulted?
   d. Did the National Security Council authorize deployment?
   e. Did DEST members act as a stand-alone advisory group to the FBI SAC?

Task# JFO-11: JFO Logistics Support	
Outcome: Emergency Management	Location: JFO
Response Element: JFO Logistics Section	Jurisdiction:
Evaluator:	Contact #:

Follow-up Analysis	
Upon completion of the day's exercise play, evaluators should compile their observations into a chronological narrative of events, describing outcomes achieved or not achieved. For any outcomes that are not achieved, the evaluator should analyze the sequence of events and attempt to determine the cause using the questions at right. The questions below may further help determine root cause.	• What happened? • What was supposed to happen? • If there is a difference, why? • What is the impact of that difference? • What should be learned from this? • What corrective actions are recommended?

1. Describe the facility selected as the JFO site.
   a. Was the facility chosen adequate for the situation at hand?
   b. Was the size structured to allow for expansion?
   c. Who on the JFO Coordination Group and the ERT-A was involved in the selection process?
   d. How long did it take to identify/obtain an adequate facility?
2. Describe the floor plan and administrative organization of the facility.
   a. Was there a posted floor plan? Was it adequate? Did it effectively map/locate sections? Were sections clearly identified by high-standing table card stands or other means?
   b. Were telephone directories prepared? Were they accessible by all sections/branches?
3. Describe the physical location of the various JFO components.
   a. Was the component virtual or physical?
   b. Where was the JOC (if applicable)? Where was the JIC? Where was the MACC (if applicable)
   c. Where were the other JFO components?
   d. Was the layout effective for interaction and communication?
   e. What type of conference/private space did the JFO Coordination Group have for meetings & VTC?
4. Describe the identification methods used by assigned section personnel.
   a. How were personnel identified (i.e., hats, vests, agency jackets, name tags, ICS color coding)?
5. Describe the JFO IT, communications systems, and administrative systems.
   a. Were there high speed faxes available? Were fax machines adequate? Assess the downtime/delay, if any, associated with sending/receiving faxes.
   b. Describe the computers used. Were the speeds/memories adequate? Were they wired/wireless? Could a member easily move to another assignment in the JFO?
   c. Was the network established suitable for the needs of the JFO?
      i. Did all who needed it have access to JFOnet?
      ii. Did members have remote access to parent agency networks/systems? Was the bandwidth utilized suitable for the workload?
      iii. Was there adequate connectivity between the JFO and other Federal, State, local, and tribal EOCs?
      iv. Were there any bugs in the system software? Repetitive log-ins, unsignalled logouts? Was the software user friendly?
   d. Was the telephone system sufficient for the staff needs? Did the system have mute capability? Headsets? Jacks? Voicemail? Labels?
6. What equipment was used to monitor news broadcasts?
7. Who was assigned as Logistics Section Chief?
   a. Describe his/her span of control.
   b. What branches/units were activated within the Logistics Section?
8. What additional supplies were used to support the JFO staff?
   a. Displays?
   b. Office supplies?
   c. Maps?
   d. Reference materials?

Task# JFO-12: Principal Federal Official	
Outcome: Emergency Management	Location: JFO
Response Element: PFO	Jurisdiction:
Evaluator:	Contact #:

Follow-up Analysis	
Upon completion of the day's exercise play, evaluators should compile their observations into a chronological narrative of events, describing outcomes achieved or not achieved. For any outcomes that are not achieved, the evaluator should analyze the sequence of events and attempt to determine the cause using the questions at right. The questions below may further help determine root cause.	• What happened? • What was supposed to happen? • If there is a difference, why? • What is the impact of that difference? • What should be learned from this? • What corrective actions are recommended?

1. After the appropriate PFO designation by the Secretary, how were the PFO support staff and support staff activated?
   a. Were the PFO support staff and staff members pre-designated personnel?
   b. Were the PFO support staff and staff members trained in and familiar with the PFO concept and JFO operations?
   c. How well did the PFO support staff and staff members interact with the JFO personnel?
   d. Did PFO support staff and staff members participate in JFO "all hands" briefings? Shift-change situational briefings?
   e. Were there adequate agency liaison officers assigned to the PFO staff?
   f. Did the PFO support staff/liaisons integrate into the JFO Coordination Staff? At what point in the incident were they detached from the PFO staff? Was there a smooth transition?

2. Was a PFO's Press Secretary appointed to the PFO support staff/JFO?
   a. Who was designated the PFO's Press Secretary? (name/title)
   b. Did the PFO's Press Secretary successfully manage the PFO's public messaging mission? Was the PFO's Press Secretary assigned collateral duties outside the PA arena? If so, did that affect operational capabilities?
   c. Was the PFO's Press Secretary the JFO JIC Manager/Director or was that responsibility delegated to a PAO? If so, how effective was the dual-hatting of the PFO's Press Secretary?
   d. Did the PFO's Press Secretary have sufficient support staff?

Task# JFO-13: External Coordination	
Outcome: Emergency Management	Location: JFO
Response Element: JFO Coordination Group	Jurisdiction:
Evaluator:	Contact #:

Follow-up Analysis	
Upon completion of the day's exercise play, evaluators should compile their observations into a chronological narrative of events, describing outcomes achieved or not achieved. For any outcomes that are not achieved, the evaluator should analyze the sequence of events and attempt to determine the cause using the questions at right. The questions below may further help determine root cause.	• What happened? • What was supposed to happen? • If there is a difference, why? • What is the impact of that difference? • What should be learned from this? • What corrective actions are recommended?

1. IIMG
   a. Did the PFO serve as the primary POC with the IIMG?
   b. In circumstances where there is only an FCO, did he/she serve as the POC with the IIMG?
   c. Was there any deviation in the PFO/FCO interaction with the IIMG Director? If so, did it adversely effect communications?
2. HSOC, HSOC/NRCC, and RRCC
   a. Did the JFO establish an effective "battle rhythm" with the HSOC/NRCC and RRCC?
   b. Which entity established the battle rhythm reporting timeline?
   c. Did the HSOC set the operations tempo? If not, why not?
   d. Did the JFO assume responsibility for coordinating emergency support functions and resource responsibilities from the RRCC and HSOC/NRCC? If so, was it done in a timely fashion?
3. HSOC/NICC
   a. Was the HSOC/NICC utilized by the JFO to share information across infrastructure and key resource sectors?
   b. Did the JFO External Affairs Officer and the JFO Coordination Staff Preparedness Liaisons maintain direct contact with the HSOC/NICC?
   c. Did the JFO, HSOC, and HSOC/NICC coordinate their communications to national-level infrastructure and resource information-sharing entities?
4. Federal Regional and Headquarters Operations Centers
   a. Did the JFO coordinate and deconflict information sharing between Federal regional and headquarters operations centers and the JFO?
   b. Did the JFO provide the SFO with direct reporting channels with their respective regional and headquarters operations centers?
5. State, Tribal, and Local EOCs
   a. Did the impacted State Emergency Management Office assign a State Coordinating Officer as liaison to the JFO/JFO Coordination Group? If not, why not?
   b. If a Stafford Act disaster declaration, did the Governor's Office assign a Governor's Authorized Representative as liaison to the JFO/JFO Coordination Group? If not, why not?
6. National and Regional Advisory Entities
   a. Did the incident warrant activation of regional and national entities? If so, was the interaction between the JFO accomplished through the cognizant SFO?
7. On-Scene Incident Command Structures
   a. Did the JFO Situation and Resources Units establish direct interaction with Federal area/incident command structures?
   b. Was this interaction effective?
   c. Did the JFO establish direct interaction with State and local area/incident command structures? If yes, why?
   d. Did the SCO lead official in the JFO act as the conduit for interaction with State incident command operations? How was this interaction accomplished? Was it effective?

Task# JFO-14: JFO Safety & Security	
Outcome: Emergency Management	Location: JFO
Response Element: JFO Security Officer	Jurisdiction:
Evaluator:	Contact #:

Follow-up Analysis	
Upon completion of the day's exercise play, evaluators should compile their observations into a chronological narrative of events, describing outcomes achieved or not achieved. For any outcomes that are not achieved, the evaluator should analyze the sequence of events and attempt to determine the cause using the questions at right. The questions below may further help determine root cause.	• What happened? • What was supposed to happen? • If there is a difference, why? • What is the impact of that difference? • What should be learned from this? • What corrective actions are recommended?

1. Did the security personnel deployed/designated by DHS Security accomplish the task at hand?
   a. How many were deployed? Which agency filled this role?
   b. Was a JFO Security Officer designated?
      i. Who designated the JFO Security Officer?
      ii. What agency filled this role?
      iii. Were any duties delegated to a Deputy Security Officer? If yes, which functions were delegated? Which agency filled this role?
   c. Were security personnel familiar with procedures and the JFO SOP Security Procedures Annex?
2. What physical security measures were implemented?
   a. Controlling access?
3. What information security measures were implemented?
   a. Were STUs/STEs compatible with other elements?
   b. Were there secure fax machines? How efficient were they? Were there enough?
   c. Were secure communications used by personnel to pass sensitive information?
   d. Were secure communications maintained and adequate for the incident scope?
   e. Was a Secure VTC available? How did it function? Was it necessary? Did it enhance information exchange?
   f. Was there a SCIF available? Was it adequate for the VTC and other secure conferences?
4. What personnel security measures were implemented?
   a. Processing clearances?
   b. Receiving clearances from member agencies?
   c. Issuing clearance-coded badges?
   d. Advising personnel to maintain badge security?
5. What operational security measures were implemented?
   a. Were there enough security containers/safes available?
   b. How were sensitive documents handled/disposed of?
6. Was the Worker Safety and Health Support Annex activated?
   a. What agency was designated to oversee/support this function?
   b. How were health and safety problems addressed?
7. Was an Emergency Action Plan developed?
   a. How was this plan shared with JFO personnel?
   b. Were personnel made aware of the COOP location?
   c. How was the plan posted?
   d. Was there a safety and security brief? Was it given to all shifts?