

## SECTION III: CAPABILITY SUMMARIES

### Capability Summary Template

#### **Capability Description**

The capability description is a statement of the principal action or activity that must be performed. Capabilities are combinations of resources that provide the means to achieve a measurable outcome resulting from performance of one or more tasks, under specified conditions and to national standards.

#### **Outcome**

Statement of the expected outcome resulting from the performance of one or more critical tasks, under specified conditions and to national standards.

#### **Relationship to National Response Plan (NRP) ESF/Annex**

Maps the capability to the National Response Plan (NRP) Emergency Support Functions (ESFs) and Annexes that are most closely associated with the capability description and outcome statement.

#### **Activities Performed with the Capability**

Key activities that would be conducted with the capability are identified. This list provides additional information to support the description and ensures that the list of critical tasks address all appropriate activities under this capability.

#### **Critical Tasks**

Lists the tasks that need to be performed to achieve the desired outcome. Critical tasks are defined as those tasks that must be performed during a major event to prevent occurrence, reduce loss of life or serious injuries, mitigate significant property damage, or are essential to the success of a homeland security mission. The first column includes the task number found in the UTL. The number incorporates a reference to the Mission and Function in the taxonomy and a sequence number. The second column identifies the task. The critical task list may include new tasks identified by the stakeholder working group or tasks that were revised. These tasks will be added to the UTL and will be assigned a UTL number.

#### **Performance Measures and Objectives**

The Performance Measures define how the demonstration of the capability through the performance of critical tasks would be measured. The Performance Objective defines how well and how quickly the task should be performed. Some measures may be outcomes while others may be outputs that serve as surrogates or indicators for outcomes.

## **Capability Elements**

Capability Elements are the resource required to perform the critical tasks, under the conditions defined by the National Planning Scenarios, to the performance standards. They include: personnel, planning, organization & leadership, equipment & systems, training, and exercises, evaluation, and corrective actions. Any combination of properly planned, organized, equipped, trained, and exercised personnel resources can be utilized to achieve the outcome. The capability elements are not an exhaustive list of requirements, but provide a guide to the type of resources that are generally required to perform the critical tasks.

## **Linked Capabilities**

Linked capabilities are those capabilities that are directly related to the subject capability and must be in place to perform tasks that feed into the capability, directly follow the capability, or that must be performed concurrently with the capability to achieve desired outcome.

## **References**

Key documents used to develop the Target Capability.

## **Capability Planning Factors and Target Levels**

Capability planning factors are the result of analysis of capability requirement by stakeholder working groups over a two month period and represent an initial effort to define national targets to develop a national network of capabilities. The appendix also includes the planning of assumptions and planning factors used to develop the national targets. The planning factors for each capability can be found in Appendix A.

## Interoperable Communications

### Capability Description

Communications interoperability is the ability of public safety and service agencies to talk within and across entities and jurisdictions via radio and associated communications systems, exchanging voice, data and/or video with one another on demand, in real time, when needed, when authorized.

### Outcome

A continuous flow of critical information is maintained as needed among multi-jurisdictional and multi-disciplinary emergency responders, command posts, agencies, and governmental officials for the duration of the emergency response operation in compliance with National Incident Management System (NIMS). To accomplish this, the jurisdiction has a continuity of operations plan for public safety communications to include the consideration of critical components, networks, support systems, personnel, and an appropriate level of redundant communications systems in the event of emergency.

### Relationship to National Response Plan ESF/Annex

Primary: ESF#2: Communications

Interoperable communications supports all Emergency Support Functions (ESFs) at the Federal, State, Local, and Tribal levels.

### Activities Performed with the Capability

Activity	Description
<b>Governance</b>	<ul style="list-style-type: none"> <li>▪ Consists of local, tribal, state, and federal entities as well as representatives from all pertinent public safety disciplines within the identified region. This governance group is critical to the success of interoperability planning.</li> <li>▪ Establishes common governing structure for solving interoperability issues that improves the policies, processes, and procedures of any major project by enhancing communication, coordination, and cooperation, establishing guidelines and principles, and reducing any internal jurisdictional conflicts.</li> <li>▪ Develops interoperability communications plan for participating entities.</li> <li>▪ Establishes agreements such as MOAs (Memorandum of Agreement), MOUs (Memorandum of Understanding).</li> <li>▪ Develops a long-term funding plan for sustainability and maintenance of communications interoperability.</li> </ul>

Activity	Description
<b>Standard Operating Procedures</b>	<ul style="list-style-type: none"> <li>Standard operating procedures (SOPs) are formal written guidelines or instructions for incident response. SOPs typically have both operational and technical components.</li> </ul>
<b>Technology</b>	<ul style="list-style-type: none"> <li>Technology refers to the equipment/infrastructure, network, support systems, and applications that public safety disciplines use to exchange critical information when responding to incidents.</li> </ul>
<b>Training/Exercises</b>	<ul style="list-style-type: none"> <li>Ensures communications support staffs are familiar with unique communication system requirements within a region and know how to use them in an incident.</li> </ul>
<b>Usage</b>	<ul style="list-style-type: none"> <li>Usage refers to how often interoperable communications technologies are used during planned events, day-to-day operations, and large-scale incidents.</li> <li>Real-time, on demand communications during emergency incidents, as well as planned events and routine daily operations as needed.</li> <li>Continuous flow of critical information between multi-jurisdictional and multi-disciplinary agencies at the Command level.</li> </ul>

**Critical Tasks**

UTL#	Task
Com.C.1 (Revised)	Develop communication plans, policies, and procedures that support required communications with all Federal, regional, state, local, tribal governments and agencies as well as voluntary agencies.
Com.C.1.1 (Revised)	Develop procedures to facilitate the exchange of <i>voice</i> and data with Federal, regional, state, local and tribal agencies as well as voluntary agencies.
Com.C.1.4	Develop supplemental and backup communications and information technology plans and procedures.
Com.C.1.4.2 (Revised)	Identify emergency communications and data requirements <i>for each stakeholder</i> .
New Task	Coordinate procurement and placement of technology communication systems based on a gap analysis of requirements versus existing capabilities.
Com.C.2	Coordinate and provide telecommunication and information technology support to Federal, regional, state, local and tribal officials and private sector.
Com.C.2.2 (Revised)	Implement plans and measures necessary to identify damaged critical infrastructure assets; repair, reconstitute, and secure <i>radio and associated communications</i> networks; and take action to protect these assets from secondary damage.

UTL#	Task
Com.C.5	Establish and maintain response communications systems.
Com.C.5.1	Implement response communications interoperability plans and protocols.
Com.C.5.2	Coordinate communications policy and procedures across response entities.
Res.A.3.2	Coordinate incident site communications within a NIMS compliant framework.
Res.A.3.4	Communicate internal incident response information.
Res.B.1.1	Provide direction, information, and/or support as appropriate to incident command (IC) or unified command (UC) and/or joint field office(s).
New Task	Design reliable, redundant, and robust communications systems for daily operations capable of quickly reconstituting normal operations in the event of disruption or destruction.
New Task	Develop a continuous improvement plan that enriches interoperable communications to provide advanced customer service, reliability, and operational effectiveness.
New Task	Complete an assessment of standard communication capabilities for the Public Safety Answering Points (PSAPs) and Public Safety Communication Centers to ensure an appropriate continuity of operations plan (COOP) is in place for public safety and service agencies' communications.
New Task	Maintain a common operating picture (COP) for real time sharing of information with all the participating entities to ensure all responder agencies are working from the same information.

\*New/Revised tasks will be added to the UTL

**Performance Measures and Objectives**

Performance Measure	Performance Objective
A multi-agency and multi- jurisdictional governance structure is in place to improve communications interoperability planning and coordination.	Yes/No
Participating entities in the governance structure have developed and will update interoperability communications plans as needed.	Yes/No
Formal agreements exist among jurisdictions and disciplines.	Yes/No
Governance committees have developed a plan to acquire and influence sustained interoperability and systems maintenance funding.	Yes/No
A regional set of communications Standard Operating Procedures (SOPs) that conform to NIMS are in place and implemented and include operational and technical elements.	Yes/No
Command and control policies are in place to achieve interoperability as	Yes/No

Performance Measure	Performance Objective
necessary.	
Interoperability policies and procedures are in place to allow information sharing between levels of government and federal installations involved in the incident as necessary.	Yes/No
Individual agencies across the jurisdictions have operable communications systems in place.	Yes/No
Appropriate levels of redundant communication systems are available.	Yes/No
All personnel are trained to operate communications systems according to their role at an incident.	Yes/No
Plans, procedures, and use of interoperable communications equipment have been exercised.	Yes/No
Interoperability systems are used in pertinent everyday activities as well as emergency incidents to ensure users are familiar with the system and routinely work in concert with one another.	Yes/No
An assessment of standard communication capabilities for the PSAPs/Public Safety Communication Centers, and Emergency Operations Centers (EOC), has been completed to ensure an appropriate continuity of operations plan (COOP) is in place for public safety and service agencies' communications.	Yes/No
A common operating picture (COP) for real time sharing of information with all the participating entities can be established as required.	Yes/No

**Capability Elements**

**Planning**

- Interoperability Communications Plans that provide governance, standard operating procedures, technology, training & exercises, and usage for each participant area
- Standard Operating Procedures that clearly articulate necessary processes and protocols to follow to achieve interoperability during an incident
- PSAP and Public Safety Communications Center COOP Plan to ensure responders understand back-up capacity protocol

**Organization and leadership**

- Formalized structured planning and governing bodies with defined authorities, missions, and responsibilities are in place
- Agreements between agencies (MOU/MOA) and coordinated decision making across agencies to ensure effective response

**Training**

- General orientation and education on interoperability equipment for all personnel who will respond to an event

- Routine use of interoperable equipment so participating area is accustomed with the equipment before an incident

#### **Equipment and Systems**

- A system-of-systems consisting of local, state, and federal components are in place that can be connected through common interface standards
- Operable communication systems for the disciplines and jurisdiction as defined by the local requirements
- DHS/SLGCP Interoperable Communications Technical Assistance Program (ICTAP) to assist localities by providing technical assistance

#### **Exercises, Evaluations, and Corrective Actions**

- Communication Tabletop Exercise
- Operational Exercise

#### **Capability Planning Factors and Target Levels**

Please proceed to the capability appendix to review the draft national target levels and assignment of responsibility for building and maintaining the capability. They are the result of analysis of capability requirements by stakeholder working groups over a two-month period and represent an initial effort to define national targets to develop a national network of capabilities. The appendix also includes the planning assumptions and planning factors used to develop the national targets. The targets will be refined through broad stakeholder review and other validation efforts.

#### **Linked Capabilities**

- Animal Health Emergency Support
- CBRNE Detection
- Citizen Preparedness and Participation
- Citizen Protection: Evacuation and/or In-place Protection
- Critical Infrastructure Protection
- Critical Resource Logistics and Distribution
- Economic and Community Recovery
- Emergency Operations Center Management
- Emergency Public Information and Warning
- Environmental Health and Vector Control
- Explosive Device Response Operations
- Fatality Management
- Firefighting Operations/Support
- Food and Agriculture Safety and Defense
- Information Gathering and Recognition of Indicators and Warnings
- Intelligence / Information Sharing and Dissemination
- Intelligence Analysis and Production
- Interoperable Communications
- Isolation and Quarantine
- Law Enforcement Investigation and Operations

- Mass Care
- Mass Prophylaxis
- Medical Supplies Management and Distribution
- Medical Surge
- Onsite Incident Management
- Planning
- Public Health Epidemiological Investigation and Lab Testing
- Public Safety and Security Response
- Responder Safety and Health
- Restoration of Lifelines
- Risk Management
- Structural Damage & Mitigation Assessment
- Triage & Pre-Hospital Treatment
- Urban Search & Rescue
- Volunteer Management & Donations
- WMD/Hazardous Materials Response and Decontamination

### References

1. Homeland Security Presidential Directive/HSPD-8, "National Preparedness". December 2003. <http://www.whitehouse.gov/news/releases/2003/12/20031217-6.html>
2. National Response Plan (NRP). Department of Homeland Security. December 2004.
3. National Incident Management System (NIMS). Department of Homeland Security. March 2004. <http://www.dhs.gov/interweb/assetlibrary/NIMS-90-web.pdf>
4. Emergency Management Accreditation Program (EMAP) Standards. September 2004. <http://www.emaponline.org/index.cfm>
5. Federal Leadership Needed to Facilitate Interoperable Communications Between First Responders; General Accountability Office. September 2004. <http://www.mipt.org/pdf/gao041057t.pdf>
6. Policy Briefing: The State and Local Role in Domestic Defense. Cohen, John D. and Hurson, John A. January 2002. [http://www.ppionline.org/documents/local\\_home\\_d.pdf](http://www.ppionline.org/documents/local_home_d.pdf)
7. National Mutual Aid and Resource Management Initiative, Resource Typing Definitions- I. Federal Emergency Management Agency, January 2004. [http://www.fema.gov/pdf/preparedness/initial\\_60\\_rtd.pdf](http://www.fema.gov/pdf/preparedness/initial_60_rtd.pdf)
8. National Association for Amateur Radio (ARRL). <http://www.arrl.org/>
9. NFPA 1221- Standard for the Installation, Maintenance and Use of Emergency Services Communications Systems. National Fire Protection Association. 2002 Edition. <http://www.nfpa.org/aboutthecodes/AboutTheCodes.asp?DocNum=1221>
10. NFPA 1561- Standard on Emergency Services Incident Management Systems. National Fire Protection Association. 2005 Edition. <http://www.nfpa.org/aboutthecodes/AboutTheCodes.asp?DocNum=1561>
11. Plan for Accelerating the Development of National Voluntary Consensus Standards for Public Safety Interoperable Communications. Report to Congress in Response to



- House Report 108-796 to the Fiscal Year 2005 Department of Homeland Security Intelligence Reform Bill. March 2005
12. Tactical Interoperable Communications Planning Guide. Department of Homeland Security, Office for Domestic Preparedness, Interoperable Communications Technical Assistance Program. April 2004.
  13. Statement of Requirements for Public Safety Wireless Communications and Interoperability Version 1.0. Department of Homeland Security, Office for Interoperability and Compatibility, SAFECOM Program. March 10, 2004.  
[http://www.safecomprogram.gov/SAFECOM/library/technology/1200\\_statementof.htm](http://www.safecomprogram.gov/SAFECOM/library/technology/1200_statementof.htm)
  14. Interoperability Continuum. Department of Homeland Security, Office for Interoperability and Compatibility, SAFECOM Program. April 2005.  
[http://www.safecomprogram.gov/SAFECOM/library/interoperabilitybasics/1229\\_interoperabilitycontinuum.htm](http://www.safecomprogram.gov/SAFECOM/library/interoperabilitybasics/1229_interoperabilitycontinuum.htm)
  15. Operational Guide for the Interoperability Continuum: Lessons Learned from RapidCom. Department of Homeland Security, Office for Interoperability and Compatibility, SAFECOM Program. Summer 2005
  16. Recommended Federal Grants Guidance Public Safety Communications & Interoperability Grants Department of Homeland Security, Office for Interoperability and Compatibility, SAFECOM Program. November 2004.  
[http://www.safecomprogram.gov/SAFECOM/library/grant/1016\\_safecomgrant.htm](http://www.safecomprogram.gov/SAFECOM/library/grant/1016_safecomgrant.htm)
  17. Statewide Communications Interoperability Planning (SCIP) Methodology. Department of Homeland Security, Office for Interoperability and Compatibility, SAFECOM Program.  
[http://www.safecomprogram.gov/SAFECOM/library/interoperabilitycasestudies/1223\\_statewidecommunications.htm](http://www.safecomprogram.gov/SAFECOM/library/interoperabilitycasestudies/1223_statewidecommunications.htm)
  18. National Task Force for Interoperability (NTFI) Guide – Why Can’t We Talk? Working Together To Bridge the Communications Gap To Save Lives. National Institute of Justice. February 2003.  
<http://www.ojp.usdoj.gov/nij/topics/commtech/ntfi/publications.htm>
  19. Department of Homeland Security (DHS) Homeland Security Preparedness Technical Assistance Program (HSPTAP), Technical Assistance Catalog, Interoperable Communications Technical Assistance Program (ICTAP), CBRNE Terrorism Prevention Technical Assistance Services #103 (PREV-103), CBRNE Terrorism Response # 214 (RESP-214), and CBRNE Terrorism Recovery #304 (RECV-304).  
[http://www.ojp.usdoj.gov/odp/ta\\_ictap.htm](http://www.ojp.usdoj.gov/odp/ta_ictap.htm)