Continuation Guidance – Budget Year Five
Attachment E
Focus Area E: Health Alert Network/Communications and Information Technology

CRITICAL CAPACITY #11: To ensure effective communications connectivity among public health departments, healthcare organizations, law enforcement organizations, public officials, and others (e.g. hospitals, physicians, pharmacies, fire departments, 911 Centers)

RECIPIENT ACTIVITIES:

1. **CRITICAL BENCHMARK #18:** Implement a plan for connectivity of key stakeholders involved in a public health detection and response including a 24/7 flow of critical health information, such as clinical data (build according to IT functions #1-3 in Appendix 4), alerts, (build according to IT Functions #7-9 in Appendix 4) and critical event data, (IT Functions #1-3 in Appendix 4), among hospital emergency departments, state and local public health officials, law enforcement, and other key participants (e.g. physicians, pharmacies, fire departments, 911 Centers) **(LINK TO CROSS CUTTING ACTIVITY *INTEROPERABILITY OF IT SYSTEMS*, Attachment H)**

2. **CRITICAL BENCHMARK #19:** Ensure, by testing and documentation, at least 90 percent of the key stakeholders involved in a public health response can receive and send critical health information including alerts and critical event data. (Build according to Appendix 4 - IT Functions and Specifications.)

3. Develop effective public health communications connectivity by identifying local health agencies to serve as model sites for training and education, support for organizational capacity building, and the creation of knowledge management systems for public health practitioners. In selecting sites, grantees should consider localities that were among the 120 cities identified in the Response to Weapons of Mass Destruction Act of 1997, are the largest population centers in the state, are state capitals, have special significance for terrorism preparedness and response (e.g., military base, strategic location, international port of entry, special population), and are not direct recipients of funding under this cooperative agreement.

4. Develop a system to enhance public health capacity for recruitment and tracking of participants, data collection, storage, and management, reporting and evaluation activities related to the National Smallpox Vaccination Program.

5. Ensure that hospitals, clinics, and other participants in the National Smallpox Vaccination Program maintain a directory of smallpox vaccination team members and are provided regular updates on implementation of program activities with appropriate technical assistance.

CRITICAL CAPACITY #12: To ensure a method of emergency communication for participants in public health emergency response that is fully redundant with standard Telecommunications (telephone, e-mail, Internet, etc.).

RECIPIENT ACTIVITIES:

1. Assess the capacity in your jurisdiction for redundant communication systems/devices (two-way radios, cell phones, voice mail boxes, satellite phones, amateur radio groups, hand radios or wireless messaging), the capacity of existing systems at the state and local level to broadcast and/or autodial to automatically distribute alerts and messages to these systems/devices, and the capacity to link to the emergency communication systems of local emergency response partners. If necessary, make improvements during this budget cycle.

2. Implement a second method of receiving critical alerts such as pagers, cell phones, voice mailboxes, or other devices to allow public health participants to receive alerts in full redundancy with e-mail.

3. Work with CDC, and as appropriate, other federal agencies, to develop and acquire high frequency and satellite voice/data communications systems between local, state, and federal partners. These systems will be standards based to ensure interoperability.

4. Collaborate with local emergency service providers to acquire technologies and utilize standards developed by CDC to develop UHF/VHF/HF data and/or voice communication capability between key Public Health Partners.

5. Develop broadcast auto-dialing voice messaging capabilities.

6. Provide for technological and staffing redundancy of critical information and communication systems to support these functions. (Build according to IT function #9 in Appendix 4.)

7. **CRITICAL BENCHMARK #20:** Routinely assess the timeliness and completeness of the redundant method of alerting, as it exists to reach participants in public health response.

CRITICAL CAPACITY #13: To ensure the ongoing protection of critical data and information systems and capabilities for continuity of operations in accordance with IT function #8 (see Appendix 4).

RECIPIENT ACTIVITIES:

1. Assess the existing capacity in your jurisdiction regarding policies and procedures for protecting and granting access to secure systems for the management of secure information, system backups, and systems redundancy. If necessary, develop a proposal for improvements during this budget cycle.

2. Perform regular independent validation and verification of Internet security, vulnerability assessment, and security and continuity of operations practices, and rapidly implement recommended remedial activities.

3. **Activities that may be considered:**

   a. Establish a firewall for the protection of critical information resources from the Internet.

   b. Implement Public Key Encryption (PKI), according to specifications in IT Function #9 (see Appendix 4) or equivalent methods of strong authentication for remote access from the Internet.

   c. Develop role-based authorization technology and processes to ensure selective authorization to information resources using technologies identified in IT Function #7 (see Appendix 4).

   d. Institute server- and client-based virus checking software to protect critical systems.

   e. Contract with an independent IT security firm to perform ongoing penetration testing and vulnerability analysis.

   f. Integrate all remote access to health department IT resources using commercial, off-the-shelf products for a single method of authentication.

   g. Implement software systems and/or servers to support Critical Capacities elsewhere in this guidance. Provide training and support on these systems to improve the ability of public health participants to effectively use them.

CRITICAL CAPACITY #14: To ensure secure electronic exchange of clinical, laboratory, environmental, and other public health information in standard formats between the computer systems of public health partners. Achieve this capacity according to the relevant IT Functions and Specifications (see Appendix 4).

RECIPIENT ACTIVITIES:

1. Assess the existing capacity in your jurisdiction to exchange electronic data in compliance with public health information and data elements exchange standards, vocabularies, and specifications as referenced in the NEDSS initiative. (Build according to IT Functions #1-9 in Appendix 4.) If necessary, develop a proposal for improvements during this budget cycle. **(LINK WITH CROSS CUTTING ACTIVITY *INTEROPERABILITY OF IT SYSTEMS*, Attachment H)**

2. **CRITICAL BENCHMARK #21:** Ensure that the technical infrastructure exists to exchange a variety of data types, including possible cases, possible contacts, specimen information, environmental sample information, lab results, facilities, and possible threat information. (Build according to IT Functions #1-9 in Appendix 4).

3. Develop firewall capabilities and Web technology and expertise to implement and maintain an XML-compliant SOAP service for the secure exchange of information over the Internet.

4. Develop systems and databases to implement the specifications, vocabularies, and standards to exchange like data with public health partners.

5. Implement message parsing technology to allow for the creation and processing of public health information messages.

6. Participate in national stakeholders meetings, data modeling activities, and joint application development sessions to help specify the data types that will be exchanged among public health partners and to understand how to implement them.

7. **(HRSA/CDC Cross-Cutting Activity)** Laboratory Data Standard
   a. **CRITICAL BENCHMARK #22:** Adopt and implement LOINC as the standard for electronic exchange of clinical laboratory results and associated clinical observations between and among public health department laboratories, hospital-based laboratories, and other entities, including collaborating academic health centers, that have a major role in responding to bioterrorism and other public health emergencies.
   b. In connection with CDC-provided technical assistance, identify areas where refinement or extension of LOINC would enhance public health emergency preparedness.

ENHANCED CAPACITY #9: To provide or participate in an emergency response management system to aid the deployment and support of response teams, the management of response resources, and the facilitation of inter-organizational communication and coordination.

RECIPIENT ACTIVITIES:

1. Assess the existing capacity in your jurisdiction related to emergency response management systems. Identify existing systems and ascertain their relevance and suitability for public health participation, including disaster simulation, logistics management, threat tracking and management, geographic mapping for visualization of events, and emergency resource provision and management. If necessary, develop a proposal for improvements during this budget cycle. **(LINK TO CROSS CUTTING ACTIVITY *INTEROPERABILITY OF IT SYSTEMS*, Attachment H)**

2. Ensure participation, training, and drilling of public health personnel in the use of an emergency response management system.

3. If an adequate system does not exist with emergency response partners, implement a commercial, off-the-shelf system for the support of these functions.

4. Train and drill public health participants in the use of existing emergency response systems.

ENHANCED CAPACITY #10: To ensure full information technology support and services.

RECIPIENT ACTIVITIES:

1. Assess the existing capacity in your jurisdiction related to the full provision of information technology support according to industry standard practices including modern software development practices, user support practices, and ongoing monitoring and maintenance of systems. If necessary, develop a proposal for improvements during this budget cycle.

2. Implement explicit arrangements/written policies for adequate network and desktop user support, including the ability of users to obtain answers to hardware and software operational questions, repair of equipment, installation of new equipment and software, administration of servers where appropriate, and other general technical support.

3. Develop technical support staff available in an industry standard ratio of one full time equivalent support person for each 60-100 workstations covered.

4. Provide critical operational support functions with less than 24-hour alternate site provision.

5. Implement software and/or systems to support critical activities elsewhere in this guidance with appropriate redundancy, systems mirroring, and/or systems fail-over to provide secure and continuous access to critical IT services.