Section I - Overview

The geographical boundary of the Boston Site's Combined Statistical Area (CSA) begins with the Boston-Cambridge-Quincy Metropolitan Statistical Area and travels north into New Hampshire to encompass the Micropolitan Statistical Areas of Laconia and Concord as well as the Manchester-Nashua Metropolitan Statistical Area. The Boston-Cambridge-Quincy Metropolitan Statistical Area boundary is bordered to its west by the Massachusetts Metropolitan Statistical Area of Worcester and bordered to its south by the New Bedford-Fall River-Providence Rhode Island Metropolitan Statistical Area.

The Boston Site contains the Metro Boston Homeland Security Region, selected in 2003 to be an Urban Area Security Initiative (UASI) Region, consisting of the Cities of Boston, Cambridge, Chelsea, Everett, Quincy, Revere, and Somerville, and the Towns of Brookline and Winthrop. The UASI Boston Region is approximately 95 square miles and according to the 2007 U.S. Census ranked 10th (Boston – Cambridge – Quincy) in the nation in population. In addition the Boston Site contains the Providence UASI of which was selected in 2007 to become an UASI Region. The Urban Area Working Group of the Metro Boston Homeland Security Region will be responsible for the overall direction and control of the Regional Catastrophic Preparedness Grant Program award to the Boston Site.

The Boston Site contains a number of critical infrastructures and high profile targets, including malls, stadiums, financial services corporations, technology and biotechnology firms, roughly 68 colleges, hospitals and other potential threat elements. In addition, several high-profile, annual events such as the Boston Marathon draw more than a million spectators and participants into the region. Several major transportation networks exist within the CSA site to include Massachusetts Bay Transportation Authority and Amtrak rail infrastructure, bus infrastructure, as well as various Ports throughout the Site including weekly Liquefied Natural Gas (LNG) deliveries which transit the Port of Boston and unload their cargo within the heart of the Region. Furthermore, the Boston Site includes Boston Logan International Airport, New England's largest transportation center, T.F. Green Airport, and Manchester Boston Regional Airport.

Project Focus

The project focus of this investment justification will be to prepare the Region to respond to a multiple simultaneous Improvised Explosive Device (IED) attack that results in a catastrophic incident. The project will be to create and implement a **Regional Operations Plan for IED Response**. Leveraging findings from the Nationwide Plan Review, planning will enforce collaboration across geographic and political boundaries, and ensure plans are comprehensive and interrelated. Terrorists have clearly demonstrated both the intent and capability to employ IEDs worldwide. This tactic has been used extensively by insurgents in both Iraq and Afghanistan to a high degree of achievement as well as with the demonstrated success of the transit bombings of Madrid in 2004 and London in 2005 (TSA, "Mass Transit Threat Assessment" February 2008.) Furthermore, intelligence estimates continue to support the conclusion that terrorists will continue to use IEDs to achieve their various objectives. (National Intelligence Estimate,

"The Terrorist Threat to the Homeland," July 2007.) As this type of threat has the potential to produce a large number of casualties and destruction to critical infrastructure within the Boston Site, a layered multi discipline, multi jurisdictional regional approach for the coordination of all hazards plans to prevent, prepare, respond and recover to such an incident is imperative, and recognized amongst the stakeholders. The key to mitigating the threat is planning. Therefore, the development of an overall comprehensive and regional all hazards Planning Program to appropriately prepare, prevent, respond and recover from a multiple simultaneous improvised explosive device attack throughout the Boston Site is required. These planning efforts will tie together the multitude of planning efforts that have been conducted throughout the Region to create a systematic and unified approach should an IED attack occur.

At its planning core, this investment will leverage findings from the Nationwide Plan Review. This initiative will allow collaboration across geographic and political boundaries of the Boston site Combined Statistical Area (CSA), and ensure plans are comprehensive and interrelated. The region plans to utilize scenario-driven catastrophic planning with support from operational and planning personnel. As a result, efforts will produce functional plans ready for immediate use, will address jurisdictional conflicts, and can be exercised rapidly after development. At the conclusion of the Investment, regional stakeholders will be armed with additional measures to counter, respond to, and recover from the threat of IED attacks.

Section II – RCPT Overview

The Boston Site is relying upon a Regional Catastrophic Planning Team (RCPT) to coordinate and manage this effort. Comprised of representatives from Massachusetts, Rhode Island and New Hampshire state and local agencies, Citizen Corps Council representatives, as well as Federal, and regional representatives, and Private Sector and Critical Infrastructure owners and operators, this group will provide strategic oversight and direction to the RCPGP projects. [Attachment A.]

The Mayor's Office of Emergency Preparedness (MOEP), in consultation with the Boston Urban Area Working Group, will serve as the project manager for the RCPT. However, each participating State will collectively work together on catastrophic preparedness planning initiatives. As a result, the RCPT will use an organizational charter to outline our organizational structure and general operating procedures. [Attachment B.] Further, each State will link Regional Catastrophic Planning activities with their state equivalent regional public safety stakeholders.

The cooperative agreement with FEMA will strengthen regional partnerships and create the building blocks for stronger response capabilities for our communities and businesses. The Federal Preparedness Coordinator (FPC) will assist in establishing and maintaining relationships with state, federal and tribal partners, and will coordinate technical assistance. The State Administrative Agency (SAA) will assist with ensuring regional coordination and integration with the appropriate state and local partners.

To effectuate the Boston site investments for the selected National Planning Scenario, each individual initiative will have a designated RCPT project manager to organize and manage the project, based on their expertise. Other RCPT participants or their subject matter expert designees will serve on regional working groups to build collaboration, identify project goals and objectives, develop project plans, present the goals and plans to the RCPT for comments and concurrence, and implement the project plan. For projects that require contractor procurement, MOEP will provide contract management including management of the bidding process and procurement of the contract on behalf of the RCPT.

The Boston Site RCPT is critical because catastrophic incidents and emergencies are typically not localized, resulting in significant impacts to large regions if not contained and managed effectively and consistently. Recent participation with FEMA, including the Regional Advisory Councils, has proven that addressing policy, planning and response from a regional perspective is effective and necessary. The RCPT will foster efforts to expand our collaboration to include other federal agencies, and continue to address cross-state policies and issues, including planning, response and resource sharing. Further, the RCPT will continue to lead by addressing the difficult issues critical to New England, and serve as a model for other multi-state partnerships.

Section III – Hazard Analysis Details

National Planning Scenario number twelve, Explosive Attack – Bombing Using Improvised Explosive Devices, has been identified as a realistic catastrophic threat within the Boston Site. Utilizing respective State Preparedness Reports, State Homeland Security Strategies as well as conducting discussions with the RCPT SMEs, this particular threat scenario was identified as a significant threat within the Region. Besides national intelligence estimates created on the federal level, much intelligence work has been conducted within the Commonwealth of Massachusetts Fusion Center and the Boston Regional Intelligence Center that identifies the need for integrated planning in responding to an IED attack (Boston Regional Intelligence Center Memorandum, April 2008). Additionally, within the Commonwealth of Massachusetts and the state of Rhode Island, the Massachusetts and Rhode Island State Police have conducted assessments of current capabilities of both plans and equipment resources to determine shortfalls across the Commonwealth when responding to such a scenario (see RI State Police Annual Report, 2007). Through these assessments within the Boston Site, it has been identified that more work in the area of coordination of assets and operations plans must be conducted to enhance prevention and response capabilities.

The efficient, effective and coordinated deployment of the region's resources when responding to multiple IED incidents is a planning priority captured by previous hazard analyses. Therefore funding within this investment justification will fund a multi jurisdictional planning effort to create a **Regional Operations Plan for IED Response** to appropriately utilize critical and limited resources during the time of need.

As the potential threat by an improvised explosive device becomes more real each year, it is imperative that jurisdictions throughout the Boston Site come together to begin preparing a regional plan that coordinates all individualistic preparation, prevention, response and recovery planning efforts throughout the multitude of jurisdictions found within the region. The coordination and integration of all plans as well as the management of resources is necessary for an effective regional response to a catastrophic incident.

Section IV – Catastrophic Planning Project

This Investment Justification will support the planning project of creating a **Regional Operations Plan for IED Response** that will enhance the Boston Site's catastrophic incident preparedness. In addition, the Regional Operations Plan for IED Response will include the following three annexes: a) Resource and Logistics; b) Mass Casualty; and c) Emergency Public Information (unified messaging).

The project goal of devising a Regional Operations Plan will be achieved by fusing the various IED related Homeland Security funded initiatives identified within the State Preparedness Reports and Federal, State, and UASI Homeland Security Strategies throughout the Region. Moreover, the project will influence and coordinate the myriad of federal, state and local plans, procedures and policies developed and implemented within the Region. Furthermore, the planning initiatives resulting from this project will provide an overall multi jurisdictional and multi discipline overview of previously identified gaps to provide a strategic planning framework for future planning and procurement efforts of the Region. Therefore, by providing this regional strategic planning framework, the initiatives funded within this particular project will complement current disparate planning initiatives on a more regional perspective to prepare the Region for a catastrophic incident.

The Regional Operations Plan for IED Response and will focus on the following: the establishment of resource management zones for response operations; resource management when responding to multiple attacks; the coordination of mass casualty response; and, the creation of a unified regional apporach towards emergency public information.

The expected outcomes of creating a Regional Operations Plan for IED Response and its incorporated three Annexes are:

Enhanced Multi-jurisdictional Collaboration. It is envisioned that both the RCPGP and the project of creating the Regional Operations Plan will promote regional efforts to break down planning silos. By establishing structures like the RCPT, long term planning can be successfully integrated throughout the Region. Most significantly, this planning approach will enhance inter and intra state relations.

Coordination with public and private organizations. If a multiple simultaneous IED attack were to occur within the Boston Site, no one public safety entity would be able to

muster the resources and personnel to respond to an incident. The ramifications and resources would lie beyond a single agency, municipality, or even state. Thus by pre-arranging plans and the coordination of government and non-governmental resources prior to an attack, the Boston Site will be prepared to effectively and appropriately marshal resources and personnel as needed to effectively respond. (The Federal Response to Hurricane Katrina: Lessons Learned, February 2006, pg. 52.) Furthermore, the development of a Regional Operations Plan will contain many public and private safety community participants, including members from academia, the medical community, and the financial sector. Participation from these entities will further enhance the regions preparedness as this planning effort will aggressively incorporate non traditional safety entities.

Development of formal regional plans. The newly created Regional Operations Plan for IED Response will create a series of formal IED prevention, response and recovery protocols. The plan will describe the general sequence of actions, supported by checklists that describe detailed actions for different threats and hazards (NPR 2, pg 13). Also included will be annexes, like a resource management annex, that will adequately describe in detail the means, organization, and process by which the Boston Site will find, obtain, allocate, track, and distribute resources to meet operational needs during an incident.

Through the development of multijurisdictional approaches, the coordination with public and private organizations, and development of formal plans, the continuum for preparedness within the Boston site is advanced. However, rather than begin with a blank slate and potentially duplicating current plans, preparedness planning regarding the Regional Operations Plan will improve upon current and past investments made throughout the Boston Site. Moreover, the various projects associated with this investment justification will complement current or previously funded HSGP planning projects throughout the entire Boston site. Many all hazard standard operating procedures and/or plans have been, or are being, developed on a department or jurisdiction wide basis but not on a multi regional or interstate level. Therefore, planning projects under this investment justification will further complement efforts by tying all procedures and plans together and creating both a comprehensive and integrated interstate and intrastate level regional plan.

Milestones

The expected Milestones for this investment justification are:

1. Formalize RCPT Charter (**April 3, 2008 – January 2009**)
2. Formalize and Implement RCPT Project Management Team and Working Groups (**January 2009**)
3. Obtain Outreach and Support From Subject Matter Experts to Support Project Management Team and Working Groups (**January 2009 – October 2009**)
4. Conduct Regional IED Attack Risk Assessment (**January 2009 - March 2009**)

5. Conduct Assessment of Current IED Attack Prevention, Detection, Response and Recovery Capabilities to Determine Shortfalls (**March 2009 - June 2009**)
6. Conduct Appendix Workshops to Obtain Necessary Regional Information (**May 2009 – July 2009**)
7. Create White Paper and Roadmap to Identify Next Steps and Resolutions (**June 2009- July 2009**)
8. Conduct Mid Term RCPT Project Review Meeting (**July 2009**)
9. Creation of a Regional Operations Plan for IED Response (**July 2009 - October 2009**)
10. Develop IED Response Appendices (**July 2009 - October 2009**)
    - Annex A: Resource and logistics
    - Annex B: Volunteer Management
    - Annex C: Emergency Public Information
11. Develop IED Response Plan of Action to Apply All-Source Resources to Address Shortfalls (**September 2009 – November 2009**)
12. Document Processes to Coordinate IED Attack Protective Action Decisions (**December 2009 – January 2010**)
13. Document Processes for Coordination of IED Attack Prevention and Protection Activities (**December 2009 – February 2010**)
14. Develop Regional Operations Plan for IED Response Memorandum of Agreements (**February 2010 – March 2010**)
15. Conduct Regional Workshops to Explain Regional Operations Plan for IED Response & Annexes (**March 2010 – May 2010**)
16. Develop Training Strategy for IED Attack (**March 2010 – May 2010**)

Project: Regional Operations Plan for IED Response - $2 Million

Challenges

The challenges to the effective implementation of this project likely will mirror many of the findings from the Madrid and London transit attacks. The findings from those attacks showed many areas where intra-sector, cross-sector and public/private partnerships worked effectively to communicate and resolve issues but also highlighted areas where planning and resource management could be improved. The following are four key challenges to the project completion of the Regional Operation Plan for IED Response:

Interagency Coordination. Interagency coordination, between local, regional, state, tribal and federal jurisdictions is a challenge. To mitigate this challenge, jurisdictions need to increase their interaction before an incident, and develop operations and coordination procedures for use during an incident. As the probability of the lack of interagency coordination occurring is high as well as the level of impacts should interagency collaboration not occur is additionally high, appropriate working groups to ensure the proper participation of RCPT members and Subject Matter Experts will be implemented to guarantee inter and intra coordination amongst the public and private safety entities of the Boston Site. Moreover, success will be measured in both the establishment and enhancement of regional partnerships (e.g. Boston Multi-modal Transportation Security Partnership) to tackle the goal of creating such a Regional Operations Plan. These efforts

will improve upon existing relationships and cultivate the concept of a "Megacommunity" where public/private/non-governmental, inter/intrastate, inter-jurisdictional/inter-agency coordination endures and blossoms in order to tackle much larger goals and problems over time.

Coordination of Response to Multiple Incidents between Public and Private Sectors. Coordination of response to multiple incidents across multiple infrastructures and between the public and private sectors remains a major challenge. At present, IED incident response amongst stakeholders within the region is generally effective in addressing single threats/attacks, and to some extent multiple threats/attack. However, most incidents are treated as individual and discrete events, and it would be a further challenge to develop an integrated situational awareness picture and cohesive impact assessment across sectors and attack vectors. As the probability of occurrence is high and the level of impact should the challenge occur is also high, success will be measured through establishment of coordinated plans, as well as inter-relationships that will be invaluable in future preparation for, and response to, cross sector IED incidents.

Contingency Planning, Risk Assessment, and Roles and Responsibilities. Formal contingency planning, risk assessment, and definition of roles and responsibilities across the entire IED incident response community must continue to be solidified. The challenge of coordinating efforts and limiting scope creep within the Boston Site, such as strategic decision making and interagency coordination of incident response in accordance with jurisdictional, state and federal level policy and procedures will need to be mitigated during the creation of the Regional Operations Plan for IED Response. Therefore, to mitigate challenges under this project, coordination will be undertaken through the RCPT to ensure the operations plan contains appropriate incident responses that are timely and well coordinated. Further, resource issues will have to be addressed at each agency's department level as the efficient and effective deployment of a jurisdiction's resources when responding to multiple IED incidents is a priority. As the probability of occurrence is high as well as the level of impact should the challenge occur is also high, success will be measured during an exercise where validation can occur on the developed Regional Operations Plan to ensure that responses are timely, well coordinated and understood.

Reliance on a small cadre of Subject Matter Experts. The challenge of identifying and having the consistent participation of appropriate subject matter experts will need to be addressed during the creation of this project. Subject Matter Experts (SMEs) will be critical in identifying the gaps and needs of the Boston Site as well as collecting the critical data necessary for the creation of the Regional Operations Plan for IED Response. The SME's will also be crucial in making key decisions and providing necessary resources for the project. As the probability of occurrence is high as well as the level of impact should the challenge occur is also high, success will be measured by the project management team and RCPT working aggressively with each jurisdiction's leadership to seek the participation of SMEs.

Section V – Project Management

To formalize the management of this particular project, a charter will be adopted that formalizes a governance structure, and defines the lines of authority, voting rights and reporting structure. The RCPT will be comprised of representatives of the Massachusetts-Rhode Island-New Hampshire Combined Statistical Area. A draft charter is submitted as Attachment B.

During the Grant period, select RCPT members will serve as the Executive Committee, and will be responsible for oversight of the various planning initiatives to be funded. In addition, task force/working groups will be created, comprised of designated regional subject matter experts (SMEs) to fulfill the investment components. SMEs will be multi-jurisdictional and multi-disciplinary, and will include government and non-government representatives. Finally, the Boston Urban Area Working Group (UAWG) will be responsible for the administration of the RCPGP, serve as the primary decision making authority for the program, and will oversee the RCPT. The Boston UAWG has a charter under which it governs. In addition, working groups will be created, comprised of designated regional subject matter experts (SMEs) to fulfill the investment components. Subject Matter Experts will be multi-jurisdictional and multi-disciplinary, and will include government and non-government representatives. For projects that require contractor procurement, MOEP will provide contract management services including management of the bidding process and procurement on behalf of the RCPT. Finally, the Boston UAWG will be responsible for the administration of the RCPGP, serve as the primary decision making authority for the program, and will oversee the RCPT. The Boston UAWG has a charter under which it governs, and utilizes working groups and investment subcommittees to fulfill its obligations.

Currently, it is envisioned that the project management of this Investment Justification will be in the form of a project management team comprised of RCPT members and Subject Matter Experts that will work and collaborate with one another in a joint fashion. In addition to the project management team, three working groups will develop the following three annexes: a.) Resource Management and Logistics; b.) Mass Casualty; and c.) Emergency Public Information. It is envisioned that the project management team responsible for the completion of the Regional Operations Plan will oversee the three annex working groups.

Finally, as the fiduciary, the City of Boston, Mayor's Office of Emergency Preparedness will capture the in kind contributions, whether personnel match, facility, equipment or supply costs, that the Boston Site meets the 25 percent cost share requirement using non federal funds.

Boston Site
Attachment C

Non Competitive RCPGP Investment Justification Milestones

Expected Milestones:

Formalize RCPT Charter (**April 3, 2008 – January 2009**)

Formalize RCPT Project Management Team and Working Groups (**January 2009**)

Obtain Outreach and Support From Subject Matter Experts to Support Project Management Team and Working Groups (**January 2009 – October 2009**)

Conduct Regional IED Attack Risk Assessment (**January 2009 - March 2009**)

Conduct Assessment of Current IED Attack Prevention, Detection, Response and Recovery Capabilities to Determine Shortfalls (**March 2009 - June 2009**)

Conduct Appendix Workshops to Obtain Regional Information (**May 2009 – July 2009**)

Create White Paper and Roadmap to Identify Next Steps and Resolutions (**June 2009-July 2009**)

Conduct Mid Term RCPT Project Review Meeting (**July 2009**)

Creation of a Regional Operations Plan for IED Response (**July 2009 - October 2009**)

Develop IED Response Appendices (**July 2009 - October 2009**)

Develop IED Response Plan of Action to Apply All-Source Resources to Address Shortfalls (**September 2009 – November 2009**)

Document Processes to Coordinate IED Attack Protective Action Decisions (**December 2009 – January 2010**)

Document Processes for Coordination of IED Attack Prevention and Protection Activities (**December 2009 – February 2010**)

Develop Regional Operations Plan for IED Response Memorandum of Agreements

(February 2010 – March 2010)

Conduct Regional Workshops to Explain Regional Operations Plan for IED Response & Annexes (**March 2010 – May 2010**)

Develop Training Strategy for IED Attack (**March 2010 – May 2010**)

Project: Regional Operations Plan for IED Response - $2 Million

Regional Operations Plan for IED Response Projects

	Tasks	% Complete	Labor/ Work	Duration	Start Date	End Date	Dependencies	Resources
Regional Operations Plan for IED Response Project								
Conduct IED Attack Risk Assessment			**775 hours**	**60 days**	**3/2/2009**	**6/1/2009**		
1	Identify, collect, and review existing IED attack risk assessment, including threats, vulnerabilities and consequences		320 hours	20 days	3/2/2009	3/27/2008		
2	Identify gaps in existing risk assessments		80 hours	10 days	3/30/2009	4/10/2009		
3	Design a comprehensive regional risk assessment for IED attacks		80 hours	6 days	4/13/2009	4/17/2009		
4	Conduct risk assessment		160 hours	10 days	4/20/2009	5/4/2009	1,2,3	
5	Develop draft IED risk assessment report		80 hours	10 days	5/5/2009	5/19/2009	4	
6	Review of draft risk assessment by regional partners and independent peer review team		40 hours	5 days	5/20/2009	5/27/2009	5	
7	Incorporate edits from regional partners and peer review		10 hours	2 days	5/28/2009	5/29/2009	6	
8	Finalize risk assessment report		5 hours	1 day	6/1/2009	6/1/2009	7	
Conduct Assessment of Current IED Attack Prevention, Detection, Response and Recovery Capabilities			**845 hours**	**63 days**	**3/2/2009**	**6/3/2009**		
9	Develop capabilities assessment survey for a select group of local, state and federal public safety agencies		120 hours	10 days	3/2/2009	3/13/2009		
10	Administer capabilities assessment survey		200 hours	15 days	3/16/2009	4/3/2009	9	
11	Conduct data analysis and develop preliminary capabilities assessment findings		250 hours	15 days	4/6/2009	4/24/2009	10	
12	Conduct regional and select on site validation workshops to review survey findings		100 hours	10 days	4/27/2009	5/8/2009	11	
13	Develop draft IED capabilities assessment		120 hours	10 days	5/11/2009	5/22/2009	12	
14	Review of draft IED capabilities assessment by regional partners and independent peer review team		40 hours	5 days	5/25/2009	5/29/2009	13	
15	Incorporate edits from regional partners and peer review		10 hours	2 days	6/1/2009	6/2/2009	14	
16	Finalize capabilities assessment report		5 hours	1 day	6/3/2009	6/3/2009	15	
Creation of Regional Operations Plan for IED Response			**4312 Hours**	**144 days**	**6/1/2009**	**5/18/2010**		
17	Collect and review existing plans, agreements, SOPs and MOUs		960 hours	30 days	6/1/2009	7/10/2009		
18	Conduct a gap analysis on current plans		360 hours	15 days	7/13/2009	7/31/2009	17	
19	Develop a Regional Operations Plan for IED Response that addresses prevention, protection, response, and recovery		2880 hours	90 days	8/3/2009	4/23/2010	18	
20	Request peer review of document		8 hours	1 day	4/26/2010	4/26/2010	19	

Regional Operations Plan for IED Response Projects								
	Tasks	% Complete	Labor/ Work	Duration	Start Date	End Date	Dependencies	Resources
Regional Operations Plan for IED Response Project								
21	Incorporate peer review comments and generate final draft		80 hours	5 days	5/4/2010	5/11/2010	20	
22	Finalize Regional Operations Plan for IED Response		16 hours	2 days	5/12/2010	5/14/2010	21	
23	Issue final plan		8 hours	1 day	5/18/2010	5/18/2010	22	
Develop Communications & Notifications Annex Project			**1406 Hours**	**82 days**	**3/1/2010**	**6/28/2010**		
24	Collect and review existing plans, agreements and MOUs		500 hours	30 days	3/1/2010	4/9/2010		
25	Conduct a gap analysis on current plans		250 hours	15 days	4/12/2010	4/30/2010	24	
26	Develop Communications & Notifications Annex		600 hours	30 days	5/3/2010	6/11/2010	25	
27	Request peer review of document		8 hours	1 day	6/14/2010	6/14/2010	26	
28	Incorporate peer review comments and generate final draft		40 hours	5 days	6/21/2010	6/25/2010	27	
29	Finalize Communications & Notifications Annex		8 hours	1 day	6/28/2010	6/28/2010	28	
Develop Emergency Public Information & Education Annex Project			**1406 Hours**	**82 days**	**3/1/2010**	**6/28/2010**		
30	Collect and review existing plans, agreements and MOUs		500 hours	30 days	3/1/2010	4/9/2010		
31	Conduct a gap analysis on current plans		250 hours	15 days	4/12/2010	4/30/2010	30	
32	Develop Emergency Public Information & Education Annex		600 hours	30 days	5/3/2010	6/11/2010	31	
33	Request peer review of document		8 hours	1 day	6/14/2010	6/14/2010	32	
34	Incorporate peer review comments and generate final draft		40 hours	5 days	6/21/2010	6/25/2010	33	
35	Finalize Emergency Public Information & Education Annex		8 hours	1 day	6/28/2010	6/28/2010	34	
Develop Regional Operations Plan for IED Response Memorandum of Agreements			**458 Hours**	**36 days**	**6/7/2010**	**7/26/2010**		
36	Collect and Review existing MOAs		250 Hours	15 days	6/7/2010	6/25/2010		
37	Identify gaps to be addressed		100 hours	10 days	6/28/2010	7/9/2010	36	
38	Create MOAs to address gaps		100 hours	10 days	7/12/2010	7/23/2010	37	
39	Finalize MOA		8 hours	1 day	7/26/2010	7/26/2010	38	
Develop Training Strategy for IED Attack			**440 hours**	**35 days**	**6/28/2010**	**8/13/2010**		
40	Conduct assessment on trainings taught in the past/currently being taught		120 hours	10 days	6/28/2010	7/9/2010		
41	Identify training gaps		80 hours	10 days	7/12/2010	7/23/2010	40	
42	Develop IED Training Strategy		240 hours	15 days	7/26/2010	8/13/2010	41	
Validate Regional Operations Plan for IED Response			**30 hours**					

Regional Operations Plan for IED Response Projects								
	Tasks	% Complete	Labor/ Work	Duration	Start Date	End Date	Dependencies	Resources
Regional Operations Plan for IED Response Project								
43	Develop a HSEEP certified scenario to test the plan		200 hours	20 days	7/5/2010	7/30/2010	23	
44	Test the plan, as developed via a HSEEP compliant tabletop exercise		70 hours	5 days	8/9/2010	8/13/2010	43	

SECTION I

Geographical Area

The geographical boundary of the Boston Site's Combined Statistical Area (CSA) begins with the Boston-Cambridge-Quincy Metropolitan Statistical Area and travels north into New Hampshire to encompass the Micropolitan Statistical Areas of Laconia and Concord as well as the Manchester-Nashua Metropolitan Statistical Area. The Boston-Cambridge-Quincy Metropolitan Statistical Area boundary is bordered to its west by the Massachusetts Metropolitan Statistical Area of Worcester and bordered to its south by the New Bedford-Fall River-Providence Rhode Island Metropolitan Statistical Area.

The Boston Site contains the Metro Boston Homeland Security Region, selected in 2003 to be an Urban Area Security Initiative (UASI) Region, consisting of the Cities of Boston, Cambridge, Chelsea, Everett, Quincy, Revere, and Somerville, and the Towns of Brookline and Winthrop. The UASI Boston Region is approximately 95 square miles and according to the 2007 U.S. Census ranked 10th (Boston – Cambridge – Quincy) in the nation in population. In addition the Boston Site contains the Providence UASI of which was selected in 2007 to become an UASI Region. Per guidance from the Federal Emergency Management Agency, the Urban Area Working Group (UAWG) of the Metro Boston Homeland Security Region will be responsible for the overall direction and control of the Regional Catastrophic Preparedness Grant Program award to the Boston Site.

The Boston Site contains a number of critical infrastructures and high profile targets, such as malls, stadiums, financial services corporations, technology and biotechnology firms, roughly 68 colleges, hospitals, and other potential threat elements. In addition, several high-profile, annual events such as the Boston Marathon draw more than a million spectators and participants into the region. Several major transportation networks exist within the CSA site to include Massachusetts Bay Transportation Authority and Amtrak rail infrastructure, bus infrastructure, as well as various Ports throughout the Site including weekly Liquefied Natural Gas (LNG) deliveries which transit the Port of Boston and unload their cargo within the heart of the Region. Furthermore, the Boston Site includes Boston Logan International Airport, New England's largest transportation center, T.F. Green Airport, and Manchester Boston Regional Airport.

Project Focus

The project focus of this Investment Justification will be to create a **Cyber Attack Coordination Plan**. According to U.S. Department of Homeland Security (DHS) Secretary Michael Chertoff, "Cyberattacks directed against critical infrastructure targets pose one of the greatest threats to national security in the post-9/11 era" (Computerworld, April 9, 2008.) Leadership within the Boston Site recognizes the potential catastrophic impact of a cyber attack, and the repercussions that might arise within the region, affecting public and private entities. Further, due to the absence of comprehensive hazard or gap analyses, the region believes that the time is appropriate to jointly work together to clearly identify current capabilities, and begin addressing the regional approach and unified response capability for a cyber attack. [Attachment A]

While a cyber attack may not result in large numbers of casualties, due to the pervasiveness of technology in the region, and its reliance within public safety and emergency operations,

significant disruptions can cause calamitous results. As a result, the gap exists for coordinated plans for accelerating delivery of the many resources and capabilities state and local authorities may need. The need is obvious because large-scale cyber incidents have the potential to "overwhelm government and private-sector resources by disrupting the Internet and/or taxing critical infrastructure information systems. Complications from disruptions of this magnitude may threaten lives, property, the economy, and national security." (National Response Framework (NRF), Cyber Incident Annex, page 2.) Further, coordinated plans also must integrate response and recovery aspects, such as continuity of operations, e.g. how do municipalities recover systems to provide continuity of services and government, or match resiliency efforts with third parties and users. Finally, a cyber attack could cripple law enforcement investigation systems, transportation sequencing; economic infrastructure; etc.

Information and data sharing has become a core component of municipal operations, whether internal between local, state and federal agencies, or external allowing the public to conduct transactions online. While external connections are assumed to be the obvious avenue for exploitation of a cyber attack, every time a municipality allows a police officer to access a headquarters booking system database via a cruiser, or to login to a comprehensive application such as the Commonwealth of Massachusetts' Statewide Information Sharing System (SWISS), new potential exposures to cyber attacks are created. Such cyber attacks could destroy the very systems that have become vital to protecting citizens from terrorism. Furthermore, data integrity can be corrupted and/or compromised jeopardizing public safety and security if unauthorized users gain access to these systems through a cyber attack and begin to enter or alter information. (See Testimony of National Intelligence Director Michael McConnell, before the U.S. Senate Armed Services Committee, February 27, 2008).

At its planning core, this investment will leverage findings from the Nationwide Plan Review, in that planning will enforce collaboration across geographic and political boundaries of the Boston site Combined Statistical Area (CSA), and ensure plans are comprehensive and interconnected. In doing so, operational and planning personnel will be included. Efforts will produce functional plans ready for immediate use, be transferrable, will address jurisdictional/sectoral conflicts, and can be exercised rapidly after development. As a result, at the conclusion of the investment, stakeholders will be armed with additional measures to counter, prevent and respond to threats against critical infrastructure from cyber attacks.

SECTION II

RCPT Overview

The Boston Site is relying upon a Regional Catastrophic Planning Team (RCPT) to coordinate and manage this effort. Comprised of representatives from Massachusetts, Rhode Island and New Hampshire state and local agencies and organizations, Citizen Corps Council representatives, as well as Federal and regional representatives, and Private Sector and Critical Infrastructure owners/operators, this group will provide oversight and direction.

RCPT participants or their subject matter expert designees will serve on project specific workgroups to build collaboration, identify broader goals and objectives, develop project plans and deliverables, present the goals and plans to the RCPT for comments and concurrence, and

implement the project plans. Such governance roles will be memorialized within a governance Charter, to include membership, voting rights, grant management, administrative functions, and funding methodologies. [Attachment B.]

The Mayor's Office of Emergency Preparedness (MOEP), in consultation with the Boston Urban Area Working Group will serve as the project manager for the RCPT. However, each participating State has pledged to collectively work together on catastrophic cyber attack preparedness planning initiatives. Further, each State will link regional catastrophic planning activities with their public safety stakeholders.

The cooperative agreement with FEMA will strengthen regional partnerships and create the building blocks for stronger response capabilities for our communities and businesses. The Federal Preparedness Coordinator (FPC) will assist in establishing and maintaining relationships with state, federal and tribal partners, and will coordinate technical assistance. The State Administrative Agency (SAA) will assist with ensuring regional coordination and integration with the appropriate state and local partners.

Current Regional Planning Effort

The Boston Site RCPT understands catastrophic incidents and emergencies are typically not localized, and may result in significant impacts to large regions if not contained and managed effectively and consistently. Recent participation with FEMA, including the Regional Advisory Councils, has proven that addressing policy, planning and response from a regional perspective is effective and necessary. The RCPT will foster efforts to expand our collaboration to include other local, state, tribal, federal agencies, non-governmental and corporate organizations, and continue to address cross-state policies and issues, including planning, response and resource sharing. Additionally, planning will consider ongoing efforts, i.e. DHS- Massachusetts Cyber Exercise . These efforts are warranted, because 'public/private partnership is easy to say, but it's very hard to do in reality . That is why communication channels must be established, tested and kept fresh well in advance of a crisis. (See Government Computer News, Lessons from Cyber Storm II, April 9, 2008). Further, the RCPT will continue to lead by addressing the difficult issues critical to New England, and serve as a model for other multi-state partnerships.

SECTION III

Hazard Analysis Details

Among the National Planning Scenarios, scenario number fifteen, Cyber Attack has been identified as one of the most realistic and urgent threats facing the Boston Site. Selection was based upon reviews of the various threat analyses available locally (via Boston Regional Intelligence Center), state-wide (e.g. New Hampshire cyber alert evaluation and planning efforts) and federally (see for example Homeland Security Threat Assessment, DHS, August, 2007). The financial losses and disruption to transportation, government services and/or economic activity associated with a cyber attack would be catastrophic. In addition, Boston Site leadership has acknowledged the lack of comprehensive hazard analysis planning underway within the region for a cyber attack, and the need for enhanced planning to respond to an cyber attack.

Over the past year, cyber exploitation activity has grown more sophisticated, more targeted, and more serious. The Intelligence Community expects these trends to continue in the coming year. (Annual Threat Assessment Testimony before the Senate Select Committee on Intelligence, Director of National Intelligence, 5 February 2008). For instance, "last May a botnet attack in Estonia essentially shut down the Estonian government for a period of time. It affected their financial system, it affected media websites, and this occurred over the course of two weeks." (Remarks by Homeland Security Secretary Michael Chertoff to the 2008 RSA Conference, April 8, 2008.) Additionally, in December 2007, a warning that the US financial system was about to be struck was posted on a prominent al-Qaeda website. The posting was enough to prompt a public caution from DHS. At the regional level, a multi-week shut down of critical infrastructure systems could result in significant disruptions to public and private sector services, and result in an economic loss to the region that would have national implications. Furthermore, the focus on a cyber attack upon information technology and communications assets continues to be a core component of the DHS Cyber Storm exercise series, and the recent establishment of the DHS Cyber Security Center.

Across the region, implementation continues unabated on interconnecting data systems to promote information sharing and leveraging communications infrastructure. The recent implementation of Check 21 to enable banks to handle more checks electronically, making check processing faster and more efficient, along with the increased reliance on direct deposit/withdrawal for financial transactions, also demonstrate this interconnectedness. At the municipal public safety level, regional efforts include the Massachusetts Statewide Information Sharing System, Rhode Island Pictometry Statewide Visual Image Information System, Metro-Boston Critical Infrastructure Management System (CIMS), the Homeland Security Information Network (HSIN), and municipal Internet Protocol (IP) Telephony deployments. However, what remains unaddressed are the vulnerabilities once these efforts are completed. These gaps reveal that more work in the area of coordination of assets and operations plans must be conducted to enhance prevention and response capabilities. Finally, such efforts will complement objectives of the National Response Framework (NRF), Cyber Annex in that "the ability of States to quickly and effectively augment local response operations may be enhanced through participation in the development of venue-specific cyber incident response plans that include a coordinated advance strategy for receiving, deploying, and/or utilizing pre-identified State resources." (Cyber Annex, Page 9).

SECTION IV: CATASTROPHIC PLANNING PROJECT

Two projects will result from planning initiatives under this investment. At the core will be a **Cyber Attack Coordination Plan**, to provide an overall multi jurisdictional and multi discipline overview of regional gaps and a strategic planning framework for future efforts. By providing such a framework, the projects and milestones that follow will complement current disparate planning efforts on a more regional perspective. For instance, coordination will build upon existing efforts such as a Rhode Island State Police project to develop a quick response team for cyber attacks and raise the preparedness of government, business, and the general public through education in computer systems and data security. Recognizing the above threats, vulnerabilities and gaps, a **Resource and Logistics Resiliency Annex** will focus on coordination and integration of resources and logistics between the public and private sectors.

Preparedness planning for a cyber attack will improve upon investments already made for prevention and protection. Various initiatives associated with this investment justification complement current or previously HSGP funded planning projects throughout the entire Boston site, including efforts detailed through State Preparedness Reports and Urban Area Homeland Security Strategies. Throughout the region, standard operating procedures and/or plans have been, or are being, developed on a department or jurisdiction wide basis but not on a multi regional or interstate level. Therefore the projects under this investment enhance these efforts by integrating all plans and procedures to create both a comprehensive and inclusive inter-state and intra-state regional plan of which all partners may utilize should a cyber attack occur.

Projects and Estimated Milestones

Project 1: Cyber Attack Coordination Plan

Through the development of multijurisdictional approaches, the coordination with public, private and non-governmental organizations, and development of formal plans, the continuum of cyber attack preparedness within the Boston site is advanced. Throughout the region, analyses have either been created or are in the process of being created to identify equipment and capability gaps to respond to a cyber attack on the state and local level. These analyses whether conducted by government or non-government actors are usually done independently. For instance, the City of Boston has currently underway an assessment to gather data regarding critical applications at each agency/department as well as the current disaster recovery capabilities that are in place. Others are collecting information regarding connectivity between key system centers, and developing capabilities to support high speed connectivity that will support mutual hosting and/or backup relationships between surrounding municipalities and with private entities. However, what is needed is a comprehensive risk/capability assessment to match gaps with resources.

To build upon National Priority 2, Expanded Regional Collaboration, and improve our collective ability to effectively respond to and recover from even the most sophisticated of cyber attacks, the Boston site must formalize the many disperate practices and protocols into standard operating procedures (SOPs) and contingency plans, clarifying the roles and responsibilities of players and organizations, and providing further training and exercises. Efforts must continue to break down planning silos to create new structures like the RCPT to promote long term catastrophic planning. Competing State Preparedness Reports and Homeland Security Strategies outline prevention and protection activities which contain respective goals and objectives. These goals and objectives influence the myriad of plans, procedures and implementing documents that are being developed. However, by looking for gaps within current planning, re-engineering generic scenarios, reducing overlaps and redundancies, and ensuring coordination and integration, the continuum of preparedness is strengthened.

As a result, to transcend a cyber attack within the region, the Boston site will move beyond fragmented solutions. Layered and synchronized approaches will be maximized to link in the personnel, best practices and lessons learned, and coordinate the respective private, non-profit, and volunteer organizations.

Project 2: Resource and Logistics Resiliency Annex to Cyber Attack Coordination Plan
National Planning Scenario Fifteen, the National Response Framework Cyber Annex, and the Cyber Storm Exercise series all emphasize the importance of the private sector in prevention, deterrence, response and recovery of a cyber attack. The reasons are two-fold. First, Cyberspace is largely owned and operated by the private sector. Second, the private sector offers much in the way of lessons learned, best practices and resources.

Effective incident management of and recovery from catastrophic cyber events requires defined coordination of a wide range of organizations and activities, including non-governmental and private entities. Coordination is mandatory to address the resulting conditions with large scale competing needs, insufficient resources, and the potential absence of functioning state and local governments. As prior DHS studies have shown, during a cyber attack, the ramifications and resources lie beyond a single agency, municipality, company, or even state. To develop long-term cyber preparedness solutions, the Boston Site must integrate resource and logistics planning efforts with its Federal, regional, State, tribal, and local partners. (Nationwide Plan Review (NPR), pg. 11.)

This Resource and Logistics Resiliency Annex will further bridge national strategies with existing local (tactical) emergency operations plans and incident action plans. The Annex will also describe the general sequence of actions, supported by checklists that detail actions for different threats, hazards and responses. (NPR 2, pg 13) In addition, the Annex will further describe in detail the means, organization, and process by which the Boston Site will find, obtain, allocate, track, and distribute resources and information to meet operational and recovery needs of a cyber attack (NPR 2 pg. 69), including the mechanisms required for continuity of operations and business continuity. Thus, by pre-arranging coordination, government and non-governmental resources can be marshaled as needed to effectively respond, further enhancing resiliency. (Federal Response to Hurricane Katrina: Lessons Learned, February 2006, pg. 52.) Finally, to ensure continuity, essential components of the Annex will include "protection of essential records, facilities, equipment, and personnel; operation of alternate facilities; and functioning of emergency communications." (NPR, pages 13-14.)

Project 1: Cyber Attack Coordination Plan [$0.75 Million]

- Milestone 1: Formalize RCPT Charter (4/3/08-1/31/09)
- Milestone 2: Convene Regional Executive Committee and Regional Working Groups (1/09)
- Milestone 3: Private sector, non-governmental organization and universities outreach (1/09)
- Milestone 4: Catalogue critical infrastructure, resources and assets (1/09-3/09)
- Milestone 5: Conduct Cyber Attack Risk Assessment (1/09-3/09)
- Milestone 6: Conduct Assessment of Current Cyber Attack Prevention, Detection, Recovery and Continuity Capabilities to Determine Shortfalls (2/09-6/09)
- Milestone 7: Finalize Regional Cyber Attack Coordination Plan (5/09-8/09)
- Milestone 8: Plan of Action to Apply All-Source Resources to Address Shortfalls (9/09-11/09)
- Milestone 9: Document Coordination of Cyber Attack Protective Action Decision (12/09-1/10)
- Milestone 10: Document Coordination of Cyber Attack Prevention and Protection (12/09-2/10)

Milestone 11: Develop Regional Cyber Attack Memorandum of Agreements (2/10-3/10)
Milestone 12: Develop Training Strategy for Cyber Attack (3/10-5/10)

Project 2: Resource and Logistics Resiliency Annex to Cyber Attack Coordination Plan [$0.5 M]
Milestone 1: Draft Annex (6/09-11/09)
Milestone 2: Final Annex (11/09-2/10)

Challenges

The challenges to the effective implementation of this project likely will mirror many of the findings from the DHS Cyber Storm I exercise. The findings from that exercise showed many areas where intra-sector, cross-sector and public/private partnerships worked effectively to communicate and resolve issues but also highlighted areas where communications and planning could be improved. The following are three key challenges for this Investment:

Interagency Coordination. Interagency coordination, between local, state and federal agencies is a challenge, i.e. getting regional personnel to meet and work together. The RCPT serves as a conduit to embrace the idea that leaders and members of organizations must deliberately come together across organizational and sectoral boundaries to reach the goals they cannot achieve alone, especially when it is clear that cyber attack issues facing us today are mutual concerns that must be addressed in a shared manner. (See Megacommunities.) Further, drawing upon Findings from Cyber Storm I Exercise Report, "Broader understanding, both within government and in the private sector, of the thresholds and ramifications of activation of these bodies will also improve interagency coordination. Specifically, the cyber community needs to better understand the readiness and security postures to be considered based on such activations, as well as the level of [governmental] engagement they imply." To mitigate this challenge, agencies need to increase their interaction before an incident, and develop operations and coordination procedures for use during an incident. Furthermore, people resources for analysis and data entry is challenging. The probability of the lack of interagency coordination occurring is high. The level of impacts should interagency collaboration not occur is also high. Success will be measured with the establishment of regional relationships, including the use of SME working groups, that while useful in tackling the single goal of cyber attack coordination, this inter- jurisdictional/inter-agency coordination also endures to take on larger regional challenges.

Contingency Planning, Risk Assessment, and Roles and Responsibilities. Formal contingency planning, risk assessment, and definition of roles and responsibilities across the entire cyber incident response community must continue to be solidified. For instance, adopting some of the themes of the recent Cyber Strom II exercise will aid in coordinating efforts within the Boston site, such as strategic decision making and interagency coordination of incident response in accordance with national level policy and procedures; information sharing relationships and communications paths for the collection and dissemination of cyber incident situational awareness, response and recovery information; and the means and processes through which to share sensitive information across boundaries and sectors without compromising proprietary or national security interests. To mitigate challenges, coordination will be undertaken through the RCPT to ensure responses are timely and coordinated, and scope creep is limited. In addition, while high level policies regarding disaster recovery/business continuity, incident response,

change management, information security, and secure handling of sensitive personal information may have been drafted, further work is required to develop umbrella policies and procedures at the functional level with adequate training to implement and support these policies and procedures. Education and resource issues will also have to be addressed at each agency's department level. The probability of occurrence is high. The level of impact should the challenge occur is high. Success will be measured during an exercise where validation can occur on the developed Plans to ensure that responses are timely and well coordinated where existing process procedures were clear and fully understood by players. (See Cyber Storm I Exercise Report.)

Correlation of Multiple Incidents between Public and Private Sectors. Correlation of multiple incidents across multiple infrastructures and between the public and private sectors remains a major challenge, especially since "we may not know immediately or for some time who caused the attack." Remarks by DHS Secretary Chertoff to the 2008 RSA Conference, April 8, 2008. At present, cyber incident response is generally effective in addressing single threats/attacks, and to some extent multiple threats/attack. However, most incidents are treated as individual and discrete events, and it is challenging to develop an integrated situational awareness picture and cohesive impact assessment across sectors and attack vectors. Such efforts will rely upon our federal partners such that the benefits of the National Cyberspace Response System are integrated into "local" actions. The probability of occurrence is high. The level of impact should the challenge occur is high. Success will be measured through establishment of coordinated plans, as well as public and private relationships that will be invaluable in future preparation for and response to cross-sector cyber incidents. (See Cyber Storm I Exercise Report.)

SECTION V: PROJECT MANAGEMENT

A charter will be adopted that formalizes a governance structure, and defines the lines of authority, voting rights and reporting structure. The RCPT will be comprised of representatives of the Massachusetts-Rhode Island-New Hampshire Combined Statistical Area. A draft charter is submitted as Attachment B.

During the Grant period, select RCPT members will serve as the Executive Committee, and will be responsible for oversight of the various planning initiatives to be funded. In addition, task force/working groups will be created, comprised of designated regional subject matter experts (SMEs) to fulfill the investment components. SMEs will be multi-jurisdictional and multi-disciplinary, and will include government and non-government representatives. Finally, the Boston Urban Area Working Group (UAWG) will be responsible for the administration of the RCPGP, serve as the primary decision making authority for the program, and will oversee the RCPT. The Boston UAWG has a charter under which it governs.

As the fiduciary, the City of Boston, Mayor's Office of Emergency Preparedness will capture the in-kind contributions, whether personnel match, facility, equipment or supply costs, such that the Boston Site meets the 25 percent cost share requirement using of non-federal funds. Finally, MOEP will provide contract management services, including management of the bidding process and procurement on behalf of the RCPT.

Attachment C

Boston Site: Cyber Attack Competitive Investment Justification
Projects and Milestones

Projects

Project 1: Cyber Attack Coordination Plan.
Through the development of multijurisdictional approaches, the coordination with public, private and non-governmental organizations, and development of formal plans, the continuum of cyber attack preparedness is advanced. Throughout the region, analyses have either been created or are in the process of being created to identify equipment and capability gaps to respond to a cyber attack on the state and local level. These analyses whether conducted by government or non-government actors are usually done independently. For instance, the City of Boston has currently underway an assessment to gather data regarding critical applications at each agency/department as well as the current disaster recovery capabilities that are in place. Others are collecting information regarding connectivity between key system centers, and developing capabilities to support high speed connectivity that will support mutual hosting and/or backup relationships between surrounding municipalities and with private entities. However, what is needed is a comprehensive risk/capability assessment to match gaps with resources.

To build upon National Priority 2, Expanded Regional Collaboration, and improve our collective ability to effectively respond to and recover from even the most sophisticated of cyber attacks, the Boston site must formalize the many disperate practices and protocols into standard operating procedures (SOPs) and contingency plans, clarifying the roles and responsibilities of players and organizations, and providing further training and exercises. Efforts must continue to break down planning silos to create new structures like the RCPT to promote long term catastrophic planning. Competing State Preparedness Reports and Homeland Security Strategies outline prevention and protection activities which contain respective goals and objectives. These goals and objectives influence the myriad of plans, procedures and implementing documents that are being developed. However, by looking for gaps within current planning, re-engineering generic scenarios, reducing overlaps and redundancies, and ensuring coordination and integration, the continuum of preparedness is strengthened.

As a result, to transcend a cyber attack within the region, the Boston site will move beyond fragmented solutions. Layered and synchronized approaches will be maximized to link in the personnel, best practices and lessons learned, and coordinate the respective private, non-profit, and volunteer organizations.

Project 2: Resource and Logistics Resiliency Annex to Cyber Attack Coordination Plan.
National Planning Scenario Fifteen, the National Response Framework Cyber Annex, and the Cyber Storm Exercise series all emphasize the importance of the private sector in prevention, deterrence, response and recovery of a cyber attack. The reasons are two-fold. First, Cyberspace is largely owned and operated by the private sector. Second, the private sector offers much in the way of lessons learned, best practices and resources.

Effective incident management of and recovery from catastrophic cyber events requires defined coordination of a wide range of organizations and activities, including non-governmental and private entities. Coordination is mandatory to address the resulting conditions with large scale competing needs, insufficient resources, and the potential absence of functioning state and local governments. As prior DHS studies have shown, during a cyber attack, the ramifications and resources lie beyond a single agency, municipality, company, or even state. Integration of resource and logistics planning efforts with its Federal, regional, State, tribal, and local partners will provide for long-term cyber preparedness. (Nationwide Plan Review (NPR), pg. 11.)

This Resource and Logistics Resiliency Annex will further bridge national strategies with existing local (tactical) emergency operations plans and incident action plans. The Annex will also describe the general sequence of actions, supported by checklists that detail actions for different threats, hazards and responses. (NPR 2, pg 13) In addition, the Annex will further describe in detail the means, organization, and process by which the Boston Site will find, obtain, allocate, track, and distribute resources and information to meet operational and recovery needs of a cyber attack (NPR 2 pg. 69), including the mechanisms required for continuity of operations and business continuity. Thus, by pre-arranging coordination, government and non-governmental resources can be marshaled as needed to effectively respond, further enhancing resiliency. (Federal Response to Hurricane Katrina: Lessons Learned, February 2006, pg. 52.) Finally, to ensure continuity, essential components of the Annex will include "protection of essential records, facilities, equipment, and personnel; operation of alternate facilities; and functioning of emergency communications." (NPR, pages 13-14.)

Milestones

Project 1: Cyber Attack Coordination Plan [$0.75 Million]

- Milestone 1: Formalize RCPT Charter (4/3/08-1/31/09)
- Milestone 2: Convene Regional Executive Committee and Regional Working Groups (1/09)
- Milestone 3: Private sector, non-governmental organization and universities outreach (1/09)
- Milestone 4: Catalogue critical infrastructure, resources and assets (1/09-3/09)
- Milestone 5: Conduct Cyber Attack Risk Assessment (1/09-3/09)
- Milestone 6: Conduct Assessment of Current Cyber Attack Prevention, Detection, Recovery and Continuity Capabilities to Determine Shortfalls (2/09-6/09)
- Milestone 7: Finalize Regional Cyber Attack Coordination Plan (5/09-8/09)
- Milestone 8: Plan of Action to Apply All-Source Resources to Address Shortfalls (9/09-11/09)
- Milestone 9: Document Coordination of Cyber Attack Protective Action Decision (12/09-1/10)
- Milestone 10: Document Coordination of Cyber Attack Prevention and Protection (12/09-2/10)
- Milestone 11: Develop Regional Cyber Attack Memorandum of Agreements (2/10-3/10)
- Milestone 12: Develop Training Strategy for Cyber Attack (3/10-5/10)

Project 2: Resource and Logistics Resiliency Annex to Cyber Attack Coordination Plan [$0.5 M]

- Milestone 1: Draft Annex (6/09-11/09)
- Milestone 2: Final Annex (11/09-2/10)

Boston Site
(includes the Boston-Worcester-Manchester, MA-RI-NH Combined Statistical Area)

Boston-Cambridge-Quincy
Concord, NH
Laconia, NH
Manchester-Nashua
Providence-New Bedford-Fall River
Worcester

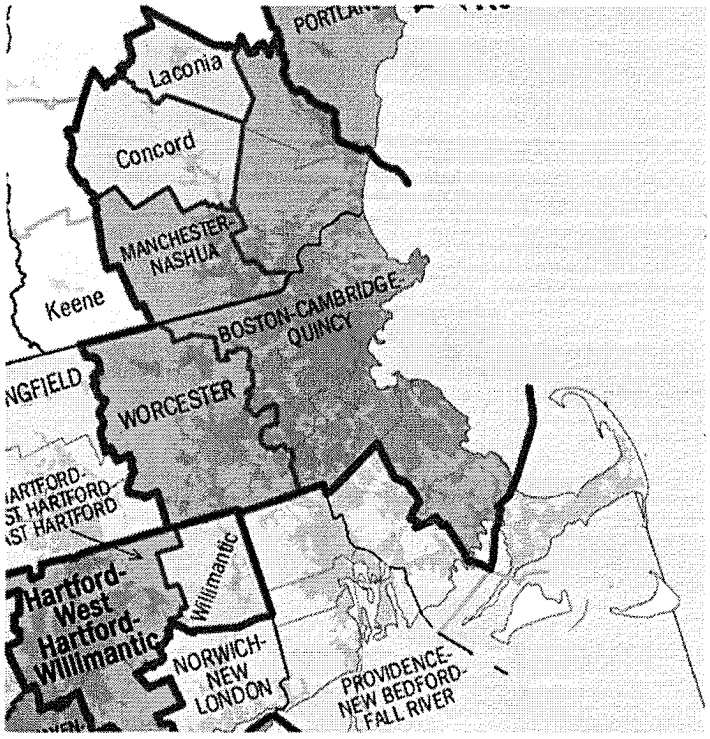

Image captured from Census.gov

Cyber Attack Coordination Project Plans

	Tasks	% Complete	Labor/ Work	Duration	Start Date	End Date	Dependencies	Resources
Cyber Attack Coordination Plan Project								
Catalogue IT/Communications Critical Infrastructure, Resources, and Assets			**862 Hours**	**70 days**	**3/2/2009**	**6/12/2009**		
1	Identify owners of IT/Communications CI/KR		120 hours	10 days	3/2/2009	3/13/2009		
2	Develop data collection plan and tool for capturing data		250 hours	20 days	3/16/2009	4/10/2009		
3	Coordinate with local, state, Federal, and private sector stakeholders to collect infrastructure data		4 hours	1 day	4/13/2009	4/13/2009		
4	Inventory, collect, and review available resources and assets related to Cyber Security		300 hours	20 days	4/14/2009	5/12/2009		
5	Identify essential services/interdependencies of CI/KR		80 hours	10 days	5/12/2009	5/26/2009		
6	Generate draft Catalogue of IT/Communications Critical Infrastructure, Resources, Assets and Services		80 hours	5 days	5/27/2009	6/1/2009	1,2,3,4,5	
7	Review of draft catalogue by regional partners and independent/peer review team		4 hours	1 day	6/2/2009	6/8/2009	6	
8	Incorporate edits from regional partners and peer review		16 hours	2 days	6/9/2009	6/11/2009	7	
9	Finalize catalogue of IT/Communications Critical Infrastructure, Resources, and Assets		8 hours	1 day	6/12/2009	6/12/2009	8	
Capabilities Assessment: ID Cyber Attack Prevention, Detection, Recovery and Continuity Capabilities			**1288 Hours**	**109 Days**	**3/2/2009**	**7/30/2009**		
10	Collect, review, and summarize sample of existing cyber-related After Action Reports (AARs)		160 hours	20 days	3/2/2009	3/27/2009		
11	Identify and document existing best practices		120 hours	10 days	3/27/2009	4/10/2009		
12	Identify legislative/regulatory aids and impediments		120 hours	10 days	4/13/2009	4/24/2009		
13	Develop capabilities assessment survey for a sample of public/private institutions across the region		200 hours	15 days	4/27/2009	5/15/2009		
14	Administer capabilities assessment survey		300 hours	20 days	5/18/2009	6/5/2009	13	
15	Conduct data analysis and develop preliminary capabilities assessment findings.		120 hours	10 days	6/8/2009	6/19/2009	10,11,12,13,14	
16	Conduct regional and select, on-site validation workshops to review survey findings		120 hours	10 days	6/19/2009	7/3/2009	15	
17	Develop draft cyber capabilities assessment report		120 hours	10 days	7/6/2009	7/17/2009	10,11,12,13,14, 15,16	

Cyber Attack Coordination Project Plans

	Tasks	% Complete	Labor/ Work	Duration	Start Date	End Date	Dependencies	Resources
18	Review of draft capabilities assessment by regional partners and independent/peer review team		4 hours	1 day	7/20/2009	7/24/2009	17	
19	Incorporate edits from regional partners and peer review		16 hours	2 days	7/27/2009	7/29/2009	18	
20	Finalize assessment report		8 hours	1 day	7/30/2009	7/30/2009	19	
Conduct Cyber Attack Risk Assessment			**748 hours**	**69 days**	**3/2/2009**	**7/1/2009**		
21	Identify, collect and review existing cyber attack risk assessment, including threats, vulnerabilities, and consequences		160 hours	20 days	3/2/2009	3/27/2009		
22	Identify gaps in existing risk assessments		120 hours	10 days	3/27/2009	4/10/2009	21	
23	Design a comprehensive regional risk assessment for cyber terrorism		200 hours	15 days	4/27/2009	5/15/2009		
24	Conduct risk assessment		120 hours	10 days	5/18/2009	6/5/2009	23	
25	Develop draft cyber risk assessment report		120 hours	10 days	6/8/2009	6/19/2009	24	
26	Review of draft risk assessment by regional partners and independent/peer review team		4 hours	1 day	6/22/2009	6/26/2009	25	
27	Incorporate edits from regional partners and peer review		16 hours	2 days	6/29/2009	6/30/2009	26	
28	Finalize risk assessment report		8 hours	1 day	7/1/2009	7/1/2009	27	
Develop Regional Cyber Attack Coordination Plan			**4108 hours**	**154 days**	**7/6/2009**	**2/12/2010**		
29	Collect and review existing plans, agreements and MOUs		720 hours	30 days	7/6/2009	8/14/2009		
30	Conduct a gap analysis on current plans		360 hours	15 days	8/17/2009	9/4/2009	29	
31	Design and conduct series of regional planning workshops		120 hours	15 days	9/7/2009	9/25/2009		
32	Develop Draft Regional Cyber Attack Coordination Plan that addresses prevention, protection, response, and recovery		2880 hours	90 days	9/28/2009	1/29/2010	9,20,28,31	
33	Review of draft coordination plan by regional partners and independent/peer review team		4 hours	1 day	2/1/2010	2/8/2010	32	
34	Incorporate edits from regional partners and peer review		16 hours	2 days	2/8/2010	2/10/2010	33	

Cyber Attack Coordination Project Plans								
	Tasks	% Complete	Labor/ Work	Duration	Start Date	End Date	Dependencies	Resources
35	Finalize Regional Coordination Plan		8 hours	1 day	2/12/2010	2/12/2010	34	
Develop Plan of Action/Strategy to Apply Resources to Existing Gaps			**56 hours**	**7 days**	**2/15/2010**	**2/24/2010**		
36	Conduct scenario-based planning workshop		40 hours	5 days	2/15/2010	2/19/2010	20,32	
37	Map how, where and when external support assets support overall response		16 hours	2 days	2/22/2010	2/24/2010	36	
Develop MOAs to Facilitate Regional Coordination			**266 hours**	**27 days**	**2/15/2010**	**3/30/2010**		
38	Identify need for MOAs to formalize Regional Coordination plan		100 hours	10 days	2/15/2010	2/26/2010		
39	Develop draft MOAs		150 hours	15 days	3/1/2010	3/19/2010	35	
40	Stakeholder/signatory review of MOAs		8 hours	1 day	3/22/2010	3/29/2010	39	
41	Finalize/Execute MOAs		8 hours	1 day	3/30/2010	3/30/2010	40	
Develop Training Strategy to Enhance Cyber Security Capabilities			**380 hours**	**40 days**	**4/5/2010**	**5/28/2010**		
42	Conduct series of planning workshops to identify training needs and develop strategy		100 hours	10 days	4/5/2010	4/16/2010		
43	Develop training strategy		200 hours	20 days	4/19/2010	5/14/2010	42	
44	Incorporate strategy into regional multi-year training and exercise plans		80 hours	10 days	5/17/2010	5/28/2010	43	
Resource and Logistics Resiliency Planning Project								
Develop Resource and Logistics Resiliency Annex			**1282 hours**	**89 days**	**3/1/2010**	**7/19/2010**		
45	Collect and review existing plans, agreements and MOUs		400 hours	25 days	3/1/2010	4/9/2010		
46	Conduct a gap analysis on current plans		200 hours	15 days	4/12/2010	4/30/2010	45	
47	Design and conduct series of regional planning workshops		150 hours	15 days	5/3/2010	5/21/2010		
48	Develop Draft Resiliency Annex		500 hours	30 days	5/24/2010	7/2/2010	47	
49	Review of draft Resiliency Annex by regional partners and independent/peer review team		8 hours	1 day	7/5/2010	7/12/2010	48	

Cyber Attack Coordination Project Plans								
	Tasks	% Complete	Labor/ Work	Duration	Start Date	End Date	Dependencies	Resources
50	Incorporate edits from regional partners and peer review		16 hours	2 days	7/13/2010	7/15/2010	49	
51	Finalize Resiliency Plan		8 hours	1 day	7/16/2010	7/19/2010	50	