COORDINATING CRITICAL TRANSPORTATION INFRASTRUCTURE VULNERABILITY ASSESSMENTS AND NEEDS PRIORITIZATION FOR THE NATIONAL CAPITAL REGION

PUBP 710 / 722 – Practicum

June 19, 2003
Prepared By:

Phil Beenhouwer
Martin Davis
Brett Graves
Matthew Hardy
Stephanie Mattes
Marvin Mmutle
Michael Nichols
Ted Smith
Tom VonWeisenstein

Under the Guidance of:

Prof. Jonathan L. Gifford, PhD.
Prof. Todd M. LaPorte, PhD.

Prepared For:

Washington Metropolitan Area Transit Authority
FORWARD

This report is the product of a student project of the School of Public Policy at George Mason University in Arlington, Virginia. Each year since 2002, students in the Master of Transportation Policy, Operations and Logistics program undertake a group project as a capstone of their program. For 2003, the practicum joined forces with a seminar on critical infrastructure protection under the sponsorship of the Critical Infrastructure Project.

These two groups of students addressed different aspects of these issues. On group examined regional transportation system vulnerability assessment and resource prioritization in the National Capital region of the District of Columbia, Northern Virginia, and Maryland. The second group examined vulnerability for tenants of commercial buildings in the Crystal City section of Arlington, Virginia, near the U.S. Pentagon.

As Director of the Master's in Transportation Policy, Operations and Logistics program, it gives me great pleasure to present this report. We greatly appreciate the cooperation of Todd M. LaPorte, the instructor of the Critical Infrastructure Seminar, and that of Kip Thomas, the research director for the Critical Infrastructure Protection Project. More information on the programs may be found at http://tpol.gmu.edu and http://techcenter.gmu.edu/programs/cipp.html.

We welcome your comments and suggestions. We also welcome suggestions for future practicum projects. We believe that such practical applications of classroom knowledge are an essential and valuable feature of our Master's program.

Jonathan L. Gifford, Director
Master's in Transportation Policy, Operations and Logistics
School of Public Policy
George Mason University
3401 North Fairfax Drive, MS 331
Arlington, Virginia 22201 U.S.A.
703.993.2280
703.993.8215 (fax)
jgifford@gmu.edu
# TABLE OF CONTENTS

1.0 INTRODUCTION .........................................................................................................................5  
1.1 CRITICAL INFRASTRUCTURE SECURITY AND THE NATIONAL CAPITAL REGION ..........5  
1.2 GUIDING PRINCIPLES ..............................................................................................................6  
   1.2.1 FEDERAL EMERGENCY MANAGEMENT ADMINISTRATION DISASTER LIFE CYCLE ....6  
   1.2.2 THE NATIONAL STRATEGY FOR THE PHYSICAL PROTECTION OF CRITICAL INFRASTRUCTURES AND KEY ASSETS .................................................................7  
   1.2.3 NATIONAL STRATEGY FOR HOMELAND SECURITY .......................................................7  
1.3 METHODOLOGY ..........................................................................................................................8  
1.4 REPORT SUMMARY ....................................................................................................................9  
1.5 ACKNOWLEDGEMENTS ...........................................................................................................9  
2.0 NATIONAL CAPITAL REGION TRANSPORTATION NETWORK ...................................10  
3.0 CATALOG OF SELF–ASSESSMENT TOOLS ...........................................................................11  
   3.1 LITERATURE SEARCH .........................................................................................................11  
   3.2 CATEGORIZATION OF TOOLS .............................................................................................13  
   3.3 ANALYSIS ...............................................................................................................................13  
4.0 REGIONAL EMERGENCY COORDINATION PLAN ..........................................................17  
   4.1 REGIONAL INCIDENT COMMUNICATIONS AND COORDINATION SYSTEM (RICCS) ...17  
   4.2 REGIONAL EMERGENCY SUPPORT FUNCTIONS (R-ESF'S) ...........................................18  
   4.3 SUPPORT ANNEXES .............................................................................................................19  
   4.4 RECP APPLICABILITY ..........................................................................................................21  
   4.5 RECP SUPPLEMENT .............................................................................................................22  
5.0 HYBRID SELF ASSESSMENT TOOL .....................................................................................23  
   5.1 HYBRID TOOL GUIDING PRINCIPLES .................................................................................23  
   5.2 PLANNING AND PREVENTION .............................................................................................23  
      5.2.1 AWARENESS ..................................................................................................................24  
      5.2.2 AGENCY MANAGEMENT ASSESSMENT .................................................................24  
      5.2.3 INTRA-AGENCY COORDINATION AND COMMUNICATION ..................................24  
      5.2.4 INTER-AGENCY COORDINATION ............................................................................25  
      5.2.5 RESOURCE ASSESSMENT .........................................................................................25
5.2.6 SECURITY MANAGEMENT ASSESSMENT ............................................................................25
5.2.7 CRITICAL ASSET ASSESSMENT ............................................................................25
5.2.8 THREAT AND VULNERABILITY ASSESSMENT .....................................................25
5.2.9 PHYSICAL SECURITY SYSTEMS ASSESSMENT ..................................................26
5.2.10 PREVENTION THROUGH ASSET HARDENING ..................................................26

5.3 RESPONSE ..................................................................................................................26
5.3.1 EMERGENCY RESPONSE CAPABILITIES ............................................................27
5.3.2 PREVIOUS EXPERIENCE ......................................................................................27
5.3.3 RESPONSE TRAINING ...........................................................................................27
5.3.4 RESOURCES ............................................................................................................27

5.4 RECOVERY ....................................................................................................................27

5.5 MITIGATION ................................................................................................................28

6.0 NEEDS PRIORITIZATION PROCESS .......................................................................29

6.1 QUANTITATIVE ..........................................................................................................29

6.2 QUALITATIVE ..............................................................................................................31
6.2.1 GOALS ACHIEVEMENT METHODOLOGY .........................................................33
6.2.2 SECURITY RISK INDEX METHODOLOGY ..........................................................38

6.3 BASELINE METHODOLOGY ....................................................................................42

7.0 FINDINGS AND RECOMMENDATIONS ....................................................................45

Appendix A: Self-Assessment Tool Summaries .......................................................... A-1
Assessing Emergency Preparedness of Transit Agencies: A Focus on Performance Indicators ..... A-2
Communication of Threats: A Guide (TCRP Report 86) ....................................................... A-4
FTA Transit Security Procedures Guide ............................................................................... A-8
Guide to Conducting Critical Asset Protection Self-Assessments (Ohio DOT)................. A-9
Integrated Transportation Analysis: Framework for Response to Natural disasters & Malevolent Attacks ........................................................................................................................................................ A-11
Making the Nation Safer: The Role of Science and Technology in Countering Terrorism .... A-12
National Infrastructure Simulation and Analysis Center (Sandia National Lab) .................. A-13
Navy Model: Infrastructure Independence & Inorganic Infrastructure Self-Assessment .... A-15
Protecting Our Transportation Systems: An Information Security Awareness Overview .... A-18
Protecting Surface Transportation Systems and Patrons from Terrorist Activities and Serious Crimes ........................................................................................................................................ A-20
## LIST OF TABLES

Table 3.1  Catalog of Self Assessment Tools .............................................................................................. 14
Table 3.2  Self-Assessment Tool Comparison ............................................................................................ 15
Table 6.1 Goals Achievement Methodology Template .................................................................................... 34
Table 6.2 Goals Achievement Methodology Sample ..................................................................................... 36
Table 6.3 Goals Achievement Methodology Sample Results ......................................................................... 38
Table 6.4 Relative Difficulty of Attack ........................................................................................................ 39
Table 6.5 Relative Severity of Attack ........................................................................................................... 39
Table 6.6 Attractiveness of Target .................................................................................................................. 40
Table 6.7 Metro Center Station SRI .............................................................................................................. 41
Table 6.8 Pentagon Station SRI ..................................................................................................................... 41
Table 6.9 Ronald Regan Nation Airport Station SRI ..................................................................................... 41
Table 6.10 Vienna Station SRI ...................................................................................................................... 42
Table 6.11 SRI Tier Index .............................................................................................................................. 42
Table 6.12 WMATA Facilities and GSA Classification System ................................................................. 44
1.0 INTRODUCTION

In November 2002 President George W. Bush signed into law the Homeland Security Act of 2002. The Act created a new Cabinet-level Agency: the Department of Homeland Security (DHS). The primary goal set forth for the agency is to protect the United States and U.S. interests abroad from terrorist attacks. In addition to the creation of the DHS, the Act requires establishment of a National Capital Region Coordinator within the Office of the Secretary of Homeland Security to oversee and coordinate Federal programs and forge relationships with State, local, and regional authorities in the National Capital Region, as defined under section 2674(f)(2) of title 10, United States Code. Among the specific responsibilities of the Coordinator is to develop an annual report to Congress that includes:

1. The resources required to fully implement homeland security efforts in the National Capital Region;
2. An assessment of the progress made by the National Capital Region in implementing homeland security efforts; and
3. Recommendations to Congress regarding the additional resources needed to fully implement homeland security efforts in the National Capital Region.1

A related initiative preceding the requirements of the Homeland Security Act and the related requirements placed on the National Capital Region by the Homeland Security Act of 2002 was the development of the Regional Emergency Coordination Plan (RECP). Under the auspices of Washington Metropolitan Area Council of Government’s (WashCOG) Ad Hoc Task Force on Homeland Security and Emergency Preparedness for the National Capital Region, the RECP provides a structure through which the National Capital Region can collaborate on planning, communication, information sharing and coordination activities before, during, and after a regional emergency. The RECP is based on the functional structure of the Federal Response Plan.2 In addition to other critical infrastructures the Plan places significant emphasis on the transportation systems in the region.

Also relevant to the security of transportation systems in the National Capital Region Washington Metropolitan Area Transit Authority (WMATA) was the subject of a vulnerability assessment that was administered by the Federal Transit Administration. However, due to security sensitivities this assessment was not made available for the purposes of this project.

1.1 CRITICAL INFRASTRUCTURE SECURITY AND THE NATIONAL CAPITAL REGION

This report focuses on developing tools that assist in conducting self-assessments and establishing regional priorities for transportation infrastructure security in the National Capital Region. This is a

---

daunting task considering how expansive and diverse the systems in the region are. Systems in the region include 14,100 lane miles of highways, more than 200 miles of carpool lanes, 103 miles of Metrorail and 162 additional miles of commuter rail. The transportation system in the National Capital region also includes an extensive bus network of local and commuter services, as well as three major airports – Reagan National, Dulles and Baltimore/Washington International. Further, the region has one of the most extensive bicycle/pedestrian trail systems in the country.3

1.2 GUIDING PRINCIPLES

The analysis and tools contained in this report were guided by three primary concepts: the Federal Emergency Management Administration (FEMA) disaster life-cycle, the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, and the National Strategy for Homeland Security.

1.2.1 Federal Emergency Management Administration Disaster Life Cycle

The FEMA disaster life-cycle describes the process through which emergency managers prepare for emergencies and disasters, respond to them when they occur, help people and institutions recover from them, mitigate their effects, reduce the risk of loss, and prevent disasters such as fires from occurring.4 Although variations of the disaster life-cycle have been defined by others, for the purposes of this report the following processes are used:

- **Planning and Prevention** - Elements of planning include communication, response training, resource assessment, multi-agency regional exercises and table top activities, and distribution of information to the media, schools, business' and individuals on what to do in the event of a disaster. Elements of prevention include physical control of facilities such as limiting access, posting personnel at key access points, promoting awareness among employees, coordinating with law enforcement to review intelligence and determine needs.

- **Response** - Involves mobilizing resources including emergency equipment, moving people away from danger, providing food, water, shelter, and medical services.

- **Recovery** - Involves developing employee tracking mechanisms, incident debriefings, and programs to help individuals manage stress associated with major disasters.

- **Mitigation** - Involves the availability of redundant resources, equipment, and systems to enable a rapid response and recovery to normal operations.

---


1.2.2 The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets

The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets identifies a clear set of national goals and objectives and outlines the guiding principles that underpin efforts to secure the infrastructure and assets, including transportation, that are vital to national security, governance, public health and safety, economy, and public confidence. Working towards achieving the goals and objectives in the Strategy also helps to meet the requirements set forth in the Homeland Security Act – especially those which are outlined for the National Capital Region Coordinator.

The Strategy groups transportation systems by modes and identifies initiatives for each mode that will help to ensure their security. Modal goals and objectives that are germane to this report include:

**Passenger Rail and Railroads**
- Improve security of intermodal transportation
- Clearly delineate roles and responsibilities regarding surge requirements

**Highways, Trucking, and Busing**
- Facilitate comprehensive risk, threat, and vulnerability assessments
- Develop guidelines and standard criteria for identifying and mitigating chokepoints
- Harden industry infrastructure against terrorism through technology

**Mass Transit**
- Identify critical planning areas and develop appropriate guidelines and standards
- Identify protective impediments and implement security enhancements
- Work with other sectors to manage unique risks resulting from interdependencies.

1.2.3 National Strategy for Homeland Security

The National Strategy for Homeland Security identifies strategies to help secure the U.S. homeland from terrorist attacks. The National Strategy for Homeland Security aligns and focuses homeland security functions into six critical mission areas, each of which are relevant to the tasks undertaken in this project. Critical mission areas include:

- intelligence and warning,
- border and transportation security,

---

• domestic counterterrorism,
• protecting critical infrastructure,
• defending against catastrophic terrorism, and
• emergency preparedness and response.6

1.3 METHODOLOGY
The work contained in this report supplements the tasks mentioned previously that have been initiated in the region, including the development of the RECP and FTA vulnerability assessments – all of which support securing the transportation infrastructure in the National Capital Region. As an example, the RECP places a strong emphasis on response planning, while this report focuses on planning related tasks. Specific tasks undertaken and documented in this report include:

1. Definition of the regional transportation systems in the National Capital Region with an emphasis placed on its importance to the economy, the multi-modal nature of the systems, and the level of integration among the various modes.

2. Conduct of a comprehensive literature search to identify infrastructure vulnerability assessment tools. Tools in this analysis are characterized as Guidance, Questionnaires, or Models.

3. Analysis of tools to evaluate their effectiveness in accommodating the processes defined in the FEMA disaster life-cycle.

4. Summarization of vulnerability assessment tasks already completed in the region. This helps to define the supplementary role that this report plays in conducting vulnerability self-assessments of the regional transportation systems.

5. Analysis of the RECP in comparison to the processes outlined in the FEMA disaster life-cycle. This helped to ensure that the tasks undertaken in this project supplement work already undertaken in the region.

6. Definition of a comprehensive vulnerability self-assessment tool that can guide WMATA and their regional transportation service partners in conducting vulnerability assessments. This tool has been developed to address each of the processes defined in the FEMA disaster life-cycle.

7. Identification of alternative methodologies for regionally prioritizing transportation security needs that are identified through the vulnerability assessment process.

---

Although the products contained in this report focus on the individual needs of WMATA, each has been structured to enable use by other transit properties and service providers from other modes – all of which will help to meet the requirements of the Homeland Security Act of 2002.

1.4 REPORT SUMMARY

Section Two provides a brief overview of the transportation systems in the National Capital Region. For the purposes of this report this summary focuses on Passenger Rail and Railroads, Highways, Trucking, Busing, and Mass Transit – as designated in the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets. Section Three provides a summary of vulnerability self-assessment tools that show potential for use in the National Capital Region. Section Four of this report provides a detailed summary of the transportation security and vulnerability assessment activities previously initiated in the National Capital Region. This section also provides an analysis of how the work contained in this report supplements work previously completed. Section Five provides a “hybrid tool’ that may be used by WMATA and other transportation service providers in the National Capital Region to conduct vulnerability self assessments. Section Six provides various methodologies for regional prioritization of needs identified by an agency. Section Seven provides key findings for the project and recommendations. Appendix A provides a brief summary of the self-assessment tools that were evaluated. Appendix B defines the criteria that was used to evaluate the self-assessment tools. Appendix C contains the hybrid vulnerability self-assessment tool.

1.5 ACKNOWLEDGEMENTS

Critical to the success of this report is both the leadership and direction of WMATA representatives Debbie Lippman, Director, Office of Intergovernmental Relations, and Fred Godine, Assistant General Manager, System Safety and Risk Protection. Activities undertaken during the development of the report have been coordinated with Ms. Lippman and Mr. Godine to best meet the needs of WMATA in conducting vulnerability self-assessments.
2.0 NATIONAL CAPITAL REGION TRANSPORTATION NETWORK

The National Capital Region is a complex area in terms of size and its political composition as a result of the number of jurisdictions and agencies that serve the area’s transportation needs. This complexity presents significant organizational and funding hurdles for the planning and coordination of emergency preparedness and response activities.

The National Capital Region is defined as the District of Columbia, Montgomery and Prince George’s counties in Maryland; Arlington, Fairfax, Loudoun, and Prince William counties in Virginia; and all cities existing within the geographic boundaries of these combined counties listed in United States Code [40 USC 71 (b)]. For consistency with the defined jurisdictions of the Washington Metropolitan Area Council of Governments (WashCOG) the term region is expanded to include Frederick County in Maryland and thus include all WashCOG member jurisdictions.7

The region covers a land area of 3,020 square miles and includes a population of 4.2 million persons (2000 Census). This area includes eighteen separate jurisdictions including the District of Columbia as well as counties and individual cities, which reside in two different states, Maryland and Virginia. The regional jurisdictions as defined by the WashCOG include: 8

- **District of Columbia**
- **Maryland**—City of Bowie, City of Gathersburg, Prince George’s County, City of College Park, City of Greenbelt, City of Rockville, Montgomery County, City of Takoma Park, Frederick County.
- **Virginia**—City of Alexandria, Fairfax County, Loudoun County, Arlington County, City of Falls Church, Prince William County, City of Fairfax, City of Manassas.

The National Capital region’s current transportation network includes 14,100 lane miles of highways, more than 200 miles of carpool lanes, 103 miles of Metrorail and 162 additional miles of commuter rail. The transportation system in the National Capital region also includes an extensive bus network or local and commuter services, as well as three major airports – Reoan National, Dulles and Baltimore/Washington International. Further, the region has one of the most extensive bicycle/pedestrian trail systems in the country.9

---


3.0 CATALOG OF SELF-ASSESSMENT TOOLS

This section provides a catalog of vulnerability self-assessment tools that show potential for use in the National Capital Region. The term “self-assessment tool” is used generically to describe any of the models (e.g., mathematical or simulation), processes or tools that may be applicable to a regional assessment of transportation infrastructure vulnerability.

The goal in identifying, cataloging and ranking these tools is to identify a set of tools that is currently available and could be used by organizations within the National Capital Region to address the requirements of the Homeland Security Act of 2002. This is not to say that a tool currently exists that will meet these needs. Rather, it is assumed that a set of tools will need to be identified that can be used in combination with each other (possibly through the creation of a hybrid tool) to begin to address Homeland Security Act of 2002 requirements and establish a process to prioritize needs throughout the region.

Fifteen tools are examined for applicability to the National Capital Region. A description of each tool is provided in Appendix A. The tools are weighed against a set of criteria that is separated into four categories: Planning and Prevention, Response, Recovery and Mitigation. An analysis of how each tool compares to the criteria is provided and each tool is categorized as one of the following: Robust, Comprehensive, Adequate or Limited for the purpose of a regional assessment of critical infrastructure vulnerability.

3.1 LITERATURE SEARCH

A literature search was conducted in order to obtain currently available vulnerability self-assessment tools. The literature searched focused primarily among the following areas:

1. Federal Transit Administration
2. Federal Highway Administration
3. National Academies: Transit Cooperative Research Program (TCRP), Nation Cooperative Highway Research Program (NCHRP) and the Transportation Research Board (TRB)
4. Homeland Security Administration
5. General Search: Lexis-Nexis, Google

A number of documents were identified based upon these sources. After a brief review of each document, fifteen of the tools appeared to be appropriate candidates for further review and analysis. It is important to note that there were some tools identified that were inaccessible because of security concerns. While it can be assumed that these tools would be applicable, they are not included in this analysis.

The tools varied from general guidance documents to an overall framework for conducting a vulnerability assessment. In order to better analyze the tools, they were classified as one of the following:
Guidance—A report or document that provides a general thought process or idea for conducting a vulnerability assessment of critical infrastructure. It does not include any detailed approach that could be applied “out-of-the-box” but must be tailored to a specific situation.

Questionnaire—A report or document that consists primarily of questions that can be answered and a self-assessment can be conducted. The questions are generic enough to not require specific tailoring to one agency or another. These types of tools are useful for a rough estimate or order of magnitude vulnerability assessment. These tools have difficulty examining specific interdependencies among systems.

Model/Framework—These tools include mathematical models and simulation programs that be used to analyze systems and the interdependencies among them. They also include a detailed framework for conducting a vulnerability assessment that can be modified to a specific agency or organization in order to conduct an analysis.

Below is a list of the fifteen tools that were analyzed and how each was classified:

**Guidance**

1. Assessing Emergency Preparedness of Transit Agencies: A Focus on Performance Indicators
3. Emergency Preparedness for Transit Terrorism (TCRP Synthesis 27)
4. Making the Nation Safer: The Role of Science and Technology in Countering Terrorism
5. Protecting Our Transportation Systems: An Information Security Awareness Overview
6. Protecting Surface Transportation Systems and Patrons from Terrorist Activities and Serious Crimes

**Questionnaire**

2. FTA Transit Security Procedures Guide
4. Navy Model: Infrastructure Independence & Inorganic Infrastructure Self-Assessment

**Model/Framework**

1. Integrated Transportation Analysis: Framework for Response to Natural Disasters and Malevolent Attacks
2. National Infrastructure Simulation and Analysis Center (SANDIA National Labs)
3. A State DOT Guide to Highway Vulnerability

3.2 CATEGORIZATION OF TOOLS

Each of the fifteen self-assessment tools was examined and ranked based upon how it addressed each of the four phases of the emergency response process: Planning and Prevention, Response, Recovery, Mitigation. Furthermore, each tool was examined to see if it incorporated a regional approach to assessing vulnerabilities or if it focused solely on one infrastructure element. Based upon these two areas, a set of 36 criteria was developed. Each of the four phases has two subgroups: Agency/Organizational needs and Resources needs. A list of the criteria is provided in Appendix B. Each of the sixteen tools was examined in detail against the criteria and was ranked using a 3-point Likert scale to determine a basic understanding of how each tool addressed the criteria. A ranking of High, Medium or Low was used and a blank cell indicates that the tool did not address the criteria at all. Below is the definition of each rank:

- **Blank**—The tool does not address the criteria
- **Low**—The tool partially addresses the criteria.
- **Med**—The tool moderately addresses the criteria.
- **High**—The tool completely addresses the criteria.

An approach was developed in order to categorize the tools. Four categorizations were chosen in order to rank the tools against each other and a set of rules were developed in order to categorize each tool as one of the four. Below are the four categories and the rules associated with each:

- **Robust**: The tool addresses all 4 Emergency Response Phases and has a minimum of 15 “high” marks
- **Comprehensive**: The tool addresses at least 3 of the 4 areas and has a minimum of 5 “high” marks
- **Adequate**: The tool addresses at least 2 of the 4 areas and has a minimum of 5 “Med” marks
- **Limited**: Those tools that do not meet the criteria above

3.3 ANALYSIS

Presented in Table 3.1 is the catalog of self-assessment tools. Each of the fifteen tools is presented as a single column and the criteria are presented in rows. The first two rows provide the classification for each tool and the categorization. Each phase of the emergency response process is separated by a shaded bar.

Seven of the fifteen tools (47%) address all four phases of the emergency response process. However, only two of those seven have sufficient “high” marks to warrant a classification as Robust. These two tools also address two of the three tool classifications covering Model/Framework and Questionnaire.
<table>
<thead>
<tr>
<th>Table 3.1 Catalog of Self Assessment Tools</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Classification</strong></td>
</tr>
<tr>
<td>Decision</td>
</tr>
<tr>
<td>-----------------</td>
</tr>
<tr>
<td><strong>Categorization</strong></td>
</tr>
<tr>
<td>Low</td>
</tr>
<tr>
<td>Moderate</td>
</tr>
<tr>
<td>High</td>
</tr>
<tr>
<td><strong>Resources</strong></td>
</tr>
<tr>
<td>Low</td>
</tr>
<tr>
<td>Moderate</td>
</tr>
<tr>
<td>High</td>
</tr>
<tr>
<td><strong>Security</strong></td>
</tr>
<tr>
<td>Low</td>
</tr>
<tr>
<td>Moderate</td>
</tr>
<tr>
<td>High</td>
</tr>
<tr>
<td><strong>Interventions</strong></td>
</tr>
<tr>
<td>Low</td>
</tr>
<tr>
<td>Moderate</td>
</tr>
<tr>
<td>High</td>
</tr>
<tr>
<td><strong>Vulnerability</strong></td>
</tr>
<tr>
<td>Low</td>
</tr>
<tr>
<td>Moderate</td>
</tr>
<tr>
<td>High</td>
</tr>
<tr>
<td><strong>Management</strong></td>
</tr>
<tr>
<td>Low</td>
</tr>
<tr>
<td>Moderate</td>
</tr>
<tr>
<td>High</td>
</tr>
<tr>
<td><strong>Disarmament</strong></td>
</tr>
<tr>
<td>Low</td>
</tr>
<tr>
<td>Moderate</td>
</tr>
<tr>
<td>High</td>
</tr>
<tr>
<td><strong>Reduction</strong></td>
</tr>
<tr>
<td>Low</td>
</tr>
<tr>
<td>Moderate</td>
</tr>
<tr>
<td>High</td>
</tr>
<tr>
<td><strong>Recovery</strong></td>
</tr>
<tr>
<td>Low</td>
</tr>
<tr>
<td>Moderate</td>
</tr>
<tr>
<td>High</td>
</tr>
<tr>
<td><strong>Resilience</strong></td>
</tr>
<tr>
<td>Low</td>
</tr>
<tr>
<td>Moderate</td>
</tr>
<tr>
<td>High</td>
</tr>
<tr>
<td><strong>Elasticity</strong></td>
</tr>
<tr>
<td>Low</td>
</tr>
<tr>
<td>Moderate</td>
</tr>
<tr>
<td>High</td>
</tr>
<tr>
<td><strong>Consequences</strong></td>
</tr>
<tr>
<td>Low</td>
</tr>
<tr>
<td>Moderate</td>
</tr>
<tr>
<td>High</td>
</tr>
<tr>
<td><strong>Elasticity</strong></td>
</tr>
<tr>
<td>Low</td>
</tr>
<tr>
<td>Moderate</td>
</tr>
<tr>
<td>High</td>
</tr>
</tbody>
</table>
Those tools categorized as Robust are:

1. Integrated Transportation Analysis: Framework for Response to Natural Disasters and Malevolent Attacks

Two of the seven tools that address all four phases were categorized as Comprehensive since they only received at least five “high” marks:

1. Emergency Preparedness for Transit Terrorism (TCRP Synthesis 27)
2. National Infrastructure Simulation and Analysis Center

One of the seven tools that address all four phases was classified as Adequate since it received at least five “Med” marks:

1. Protecting Surface Transportation Systems and Patrons from Terrorist Activities and Serous Crimes

Finally, the remaining two tools that address all four phases were classified as Limited since they received less than five “Med” marks:

1. Making the Nation Safer: The Role of Science and Technology in Countering Terrorism

The remaining eight tools address either two or three of the four phases. Two were categorized as Comprehensive and the remaining six as Limited. Table 3.2 provides a comparison between Classification and Categorization.

<table>
<thead>
<tr>
<th></th>
<th>Robust</th>
<th>Comprehensive</th>
<th>Adequate</th>
<th>Limited</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guidance</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>4</td>
<td>6</td>
</tr>
<tr>
<td>Questionnaire</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>4</td>
<td>6</td>
</tr>
<tr>
<td>Model/Framework</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>2</strong></td>
<td><strong>4</strong></td>
<td><strong>1</strong></td>
<td><strong>8</strong></td>
<td><strong>15</strong></td>
</tr>
</tbody>
</table>

Overall, the self-assessment tools that were examined provide good coverage among the three classifications (Guidance, Questionnaire, and Model/Framework). One area that the ranking of the tools did not cover is the cost or resources associated with a tool which will have an impact on utilizing certain tools. For example, the Model/Framework tools fared especially well with all three being classified as either Robust or Comprehensive. However, utilizing these tools to their fullest extent will require great effort, resources and time. Also, while the Questionnaires may be useful, it is difficult to get an understanding of a regional assessment and obtain a thorough understanding of
the interdependencies among the systems with a simple questionnaire. In addition, the Questionnaires are generally geared towards single agency (stove pipe) analysis.

Different aspects of the fifteen tools examined will form a foundation for the creation of a Hybrid Tool that is presented in Section 5.0. The Hybrid Tool will assist localities in conducting a vulnerability self assessment and begin to prioritize regional needs within the National Capital Region. The Hybrid Tool attempts to complement the WashCOG Regional Emergency Coordination Plan that is presented in the following section.
4.0 REGIONAL EMERGENCY COORDINATION PLAN

During the literature search of vulnerability assessment tools, the research team identified a regional effort that provided a framework for addressing regional emergencies. This document was prepared by WashCOG and was developed prior to the enactment of the Homeland Security Act of 2002. WashCOG created the Task Force on Homeland Security and Emergency Preparedness for the National Capital Region in October, 2001. This Task Force began the work of developing a tool to assist the local, state and federal sector partners to coordinate their response to regional emergencies. The Task Force submitted the framework for the Regional Emergency Coordination Plan (RECP) at the COG Board on April 10, 2002; which was unanimously approved. In addition, the COG board also approved the draft Memorandum of Understanding (MOU) for Development and Maintenance of the RECP for the National Capital Region, and for utilization of a Regional Incident Communication and Coordination System (RICCS). The RECP, through the signature on the MOU’s, is the agreed plan in the event of a regional emergency since September 11, 2002.

The RECP is comprised of the RICCS, the 15 Regional Emergency Support Functions (R-ESFs), and 11 Support Annexes. The RECP is designed to be a dynamic, flexible document that will change and mature with each update, reflecting its challenge to be tested through real world operations and simulations exercises.

4.1 REGIONAL INCIDENT COMMUNICATIONS AND COORDINATION SYSTEM (RICCS)

The RICCS provides a system for COG members, the State of Maryland, the Commonwealth of Virginia, the federal government, public agencies, the private sector and volunteer organizations, and schools and universities to collaborate in planning, communication, information sharing, and coordination activities before, during, and after a regional incident or regional emergency.

Based on the threat level, local, state, and federal agencies will implement appropriate protective measures. The RICCS is a tool that can be used to share information regionally about what protective measures have been taken. The RICCS is a virtual system with multiple capabilities that was designed to facilitate regional communication. Participating organizations will use multiple means of communication, including conference calling, secure websites, and wireless communication systems.

12 Ibid, page xi, paragraph 2.
13 Ibid, page xi, paragraph 2.
14 Ibid, page xv, paragraph 5, (1).
15 Ibid, page xii, paragraph 3.
16 Ibid, page Executive Summary 2, paragraph 6
17 Ibid, page Executive Summary 3, paragraph 1.
The RICCS is not intended to supersede, replace, or duplicate the existing communications and information sharing that routinely occurs among federal, state, and local emergency management organizations. Rather, it is intended to focus on information and coordination from the regional perspective.\footnote{Ibid, page Executive Summary 3, paragraph 2.}

### 4.2 REGIONAL EMERGENCY SUPPORT FUNCTIONS (R-ESF’S)

An R-ESF is a basic function shared by all jurisdictions. Individual R-ESFs identify organizations with resources and capabilities for a particular type of assistance or requirement frequently needed in a large-scale emergency or disaster. Each of the R-ESFs uses the same format to identify participant organizations, establish basic policies and planning assumptions that will guide activities, and explain how they will communicate and coordinate with each other and with other regional partners. A short synopsis of the content of each R-ESF to be used before, during, and after a regional incident or regional emergency follows:\footnote{Ibid, page Executive Summary 3-5.}

- **R-ESF #1: Transportation**—facilitates communication and coordination among regional jurisdictions and agencies concerning regional transportation issues and activities before, during, and after a regional incident or emergency.

- **R-ESF #2: Communications Infrastructure**—ensures the coordination and communication of information concerning hardware and capacity for interoperability.

- **R-ESF #3: Public Works and Engineering**—ensures an effective and timely response to regional public emergencies concerning regional water supply (including potable water and ice), wastewater (including wastewater treatment), and solid waste and debris management.

- **R-ESF #4: Fire, Technical Rescue, and Hazardous Materials Operations**—facilitates communication and coordination among regional jurisdictions concerning regional firefighting and EMS, technical rescue, and hazardous materials operations issues and activities. Note: R-ESFs #4, #9, and #10 are structurally the same and are all contained in R-ESF #4.

- **R-ESF #5: Information and Planning**—facilitates the collection, processing, and dissemination of information among regional jurisdictions and organizations. This function enhances substantive regional dialogue and communication by facilitating information sharing with all of the R-ESFs, and others as necessary, in an integrated and coordinated manner.

- **R-ESF #6: Mass Care**—promotes and ensures a coordinated regional capability to provide mass care assistance to victims that have been impacted by a regional incident or regional emergency, including a weapons of mass destruction event.
- **R-ESF #7: Resource Support**—facilitates communication and support among regional jurisdictions to assist in the effective and timely coordination of resources following an emergency.

- **R-ESF #8: Health, Mental Health, and Medical Services**—facilitates communication, cooperation, and coordination among local and state jurisdictions and a vast array of hospitals, social workers, and private-practice physicians concerning regional health, mental health, and medical services issues and activities.

- **R-ESF #9: Technical Rescue**—R-ESFs #4, #9, and #10 are structurally the same and are all contained in R-ESF #4.

- **R-ESF #10: Hazardous Materials**—R-ESFs #4, #9, and #10 are structurally the same and are all contained in R-ESF #4.

- **R-ESF #11: Food**—facilitates the procurement, storage, transportation, and distribution of food provisions and food stamps and also feeding assistance. R-ESF #11 works in conjunction with and in continuance of the mass-feeding activities performed under R-ESF #6: Mass Care.

- **R-ESF #12: Energy**—ensures an effective and timely response to public emergencies that affect the regional energy infrastructure (including the supply and delivery of electricity, natural gas, and petroleum fuels).

- **R-ESF #13: Law Enforcement**—facilitates communication and information coordination among regional jurisdictions concerning law enforcement issues and activities.

- **R-ESF #14: Media Relations and Communications Outreach**—provides accurate, authoritative, and timely regional information to news media representatives, thereby supporting other regional partners as they work to protect the health and safety of citizens.

- **R-ESF #15: Donations and Volunteer Management**—facilitates the communications and coordination among regional jurisdictions and agencies regarding the need for and availability of donations and volunteer services.

### 4.3 SUPPORT ANNEXES

To augment the RICCS, 11 Support Annexes will provide detailed information on specific topics. The Support Annexes include descriptive briefs on the following:20

(1) **Animal Protection**—lists the governmental, private sector, and nongovernmental agencies involved; the need and purpose for this function; the situations and conditions for this function; the planning assumptions, the coordination capability; and the responsibilities of the participant organizations.

---

20 Ibid, page Executive Summary, pages 5-6.
(2) **Business Continuity**—identifies the impact of potential loss of services in the event of a regional incident or regional emergency; formulates and implements viable recovery strategies; develops recovery plan(s) to ensure continuity of organizational services; and administers a comprehensive training, testing, and maintenance program. This Support Annex will be developed at a later date.

(3) **Credentialing**—provides an overview of actions taken to date regarding credentialing protocols within the National Capital Region to ensure proper access to an incident or emergency site by authorized individuals.

(4) **Disease Surveillance**—discusses the governmental and private sector health organizations; purposes and policies; description of the situation, including regional emergency conditions and planning assumptions; concept of coordination; responsibilities of the participating and supporting agencies; the preparedness cycle; and an analysis of legal issues and recommended action. This Support Annex is currently in draft form.

(5) **Economic Recovery**—provides additional communication and coordination mechanisms that may be applied when the impact of an emergency requires a coordinated effort among member jurisdictions and other stakeholders for regional economic recovery. Work is ongoing on this Support Annex.

(6) **Regional Emergency Evacuation Transportation Coordination Annex**—addresses the transportation aspects of moving people out of affected areas of the region and moving required resources into affected areas in anticipation of, and following a regional incident or regional emergency that requires large-scale evacuation. Work is ongoing on this Support Annex.

(7) **National Pharmaceutical Stockpile**—lists the local governmental and private sector health organizations in the region; the purpose and scope of the stockpile; policies, regional situation, including emergency conditions and planning assumptions; concept of coordination; responsibilities of the participating and supporting agencies; and the preparedness cycle.

(8) **Solid Waste and Debris Management**—addresses detailed issues including staging areas; mutual aid agreements; review of available resources; review of contracts already in place; requirements of regulatory agencies; monitoring data; contamination implications (i.e., biomedical, radioactive, and identifying locations/facilities that can accept contaminated waste); and disposal infrastructure/waste stream capacity and who controls that capacity. This Support Annex will be developed at a later date.

(9) **Protective Actions**—identifies steps taken to preserve the health and safety of emergency responders and the public during a public emergency and provides a framework under which the COG jurisdictions can coordinate their decisions. This support annex will be developed at a later date.

(10) **Terrorism**—addresses the unique communication and coordination aspects of dealing with a terrorist act and the crisis and consequence management relationships involved.
(11) **Water Supply Emergency Plan**—describes the 2002 Water Supply Emergency Plan and how it would effect communication and coordination regarding water supply in the event of a regional incident or regional emergency.

### 4.4 RECP APPLICABILITY

The FEMA Disaster Life Cycle, discussed in Section 1.2.1, presented four processes: Planning and Prevention, Response, Recovery and Mitigation. In the research and analysis of the RECP, the following were identified as strengths and weaknesses relating to each of the four processes.

#### Planning and Prevention

- **Communication Planning**—The RECP, utilizing the RICCS system, is a well-designed and implemented communication system for use during regional emergency response and coordinating response quickly and efficiently.

- **Front-end Planning**—The RECP establishes a good framework for each of the R-ESF's to develop their own planning, training and evaluation. However, there is no detail in any of the R-ESF's detailing how planning and training will be conducted. The flexibility built into the RECP allows for robust modifications. But, as adopted, each agency within each R-ESF's is left to determine their own methodology for planning, training and evaluating a response to an emergency situation.

#### Response

- **Regional Coordination**—The RECP firmly establishes one method for the identification, assistance and multilateral cooperation among all 17 jurisdictions within the region. This is the first plan of this magnitude that has been adopted across the country.

- **Regional Response**—The RECP was developed specifically for this purpose. The RECP provides a mechanism for a fast, regional response to an emergency situation within the region.

#### Recovery

- **Regional Recovery**—The RECP does offer limited information on Liability and Indemnification in Appendix F, but otherwise there is no mention or plan provided on recovery after an emergency situation has abated.

#### Mitigation

- **Disaster Mitigation**—The RECP does reference in some of the R-ESF's that agencies should do self assessments, but there is no unified or baseline plan provided on how agencies should prioritize mitigating their operations to minimize damage from emergency situations.

- **Risk Reduction**—The RECP details in the "Regional Emergency Evacuation Transportation Coordination Annex" the transportation issues of moving people in and around the region following a regional emergency. This annex provides a risk assessment
matrix, a general evacuation worksheet, and a detailed description of strategies that could be employed at the time of the emergency. This annex also provides five sample scenarios to provide an understanding of how this works. The RECP does not list risk reduction methods or plans for any of the other subject areas at this time.

4.5 RECP SUPPLEMENT

Clearly the RECP is a document that contributes significantly to the preparedness of the region in the event of a region-wide emergency. In fact, it is apparent that this document should serve as a foundation to other efforts that attempt to address the requirements of the Homeland Security Act of 2002 that have been set forth for the National Capital Region.

To that end, products provided in this document are a supplement to the RECP. The Hybrid Tool (presented in Section 5.0) is a gathering of salient points from the more robust tools identified in Section 3.0. Among the fifteen self-assessment tools, RECP, and the Hybrid Tool, it is thought that all aspects of the FEMA disaster life-cycle are addressed and that these tools will serve as a mechanism to identify regional needs. What is missing from the RECP and the tools is a method to assess and prioritize regional needs therefore addressing the requirements of the Homeland Security Act of 2002 for the National Capital Region. Section 6.0, Needs Prioritization Process, will address this issue.
5.0 HYBRID SELF ASSESSMENT TOOL

This section will define the assessment tool that has been developed for critical infrastructure assessments in the National Capital Region, as well as what factors guided in its development.

5.1 HYBRID TOOL GUIDING PRINCIPLES

The Hybrid Tool was developed in the context of the principles of the FEMA disaster life-cycle process. These four stages are defined in Section 1.2.1. As stated in Section 3.0, fifteen tools were examined for applicability to the National Capital Region and it was decided that none of the tools adequately addressed the needs according to the Homeland Security Act of 2002. Therefore a Hybrid Tool was formulated that is robust, comprehensive, and adequate to be applied to a regional assessment of transportation infrastructure vulnerability to meet the requirements of the Homeland Security Act of 2002 for the National Capital Region.

For optimum effectiveness, the tool has been designed as a checklist for the transit agency management to do a self-assessment. From this self-assessment, an organization can determine its needs based on the shortcomings identified while conducting the self assessment. For example, the way an organization answers the questions about its reliance on commercially-provided communications or power will tell a lot about the need for redundant support. The way an organization answers the questions in the “Asset Hardening” section will tell a lot about the need to increase perimeter security. Knowing the answers to the Hybrid Tool questions will provide insight into an organization’s needs. Section 6 presents methodologies with which to prioritize these needs.

The questions used to fashion the Hybrid Tool were formulated from:

1. Ohio Department of Transportation: Guide to Conducting Critical Asset Protection Self-Assessments;
2. Emergency Preparedness for Transit Terrorism (TCRP Synthesis 27);
3. Navy Model (Self-Assessment Questionnaire for Infrastructure Independence + Inorganic Infrastructure Self-Assessment; and

It is necessary to mention each category and its relevance to the assessment.

5.2 PLANNING AND PREVENTION

Proper preparation can facilitate coordinated action for improving response and recovery. Elements of planning include communication, response training, resource assessment, multi-agency regional exercises and table-top activities, and distribution of information to the media, schools, business’ and individuals on what to do in the event of a disaster.
Preventing an event or disaster can include three elements deterrence, detection, and defending. These elements include physical control of facilities such as limiting access, posting personnel at key access points, promoting awareness among employees, coordinating with law enforcement to review intelligence and determine needs. These countermeasures based on the perceived need level.

The Planning and Prevention category is sub-divided into:

A. Awareness
B. Agency Management Assessment
C. Intra-Agency Coordination and Communication
D. Inter-Agency Coordination,
E. Resource Assessment
F. Security Management Assessment,
G. Critical Asset Assessment,
H. Threat and Vulnerability Assessment
I. Physical Security Systems Assessment
J. Prevention through Asset Hardening

5.2.1 Awareness

Awareness as a self-assessment category is important to the transit agency because it is necessary to be aware of warnings and threats that the local law enforcement receives as well as the threat condition or level of threat as determined by the Homeland Security Administration. The tool emphasizes the need to be aware and possibly assigning a staff member to monitor and disseminate information to agency management.

5.2.2 Agency Management Assessment

The questions listed under Agency Management Assessment category ask management to accept the responsibility of security vulnerabilities and make adjustments where necessary.

5.2.3 Intra-Agency Coordination and Communication

The Intra-Agency Coordination and Communication sub-category is a unique feature of this tool because it addresses the needs for the multiple departments within an agency to work together. We believe that it is necessary that the tool address this issue because it is usually overlooked in most...
plans. The planning process should include representatives from all the departments that play a role in ensuring the security and emergency preparedness of the transit system.

### 5.2.4 Inter-Agency Coordination

The Inter-Agency Coordination category is another unique feature of this tool because most agencies do not consider the broader picture that they are part of a larger system and all planning should incorporate other systems. In one jurisdiction there are usually many other transit agencies with overlapping systems and which should be taken into account when plans are developed.

### 5.2.5 Resource Assessment

The Resource Assessment category asks the agency to assess the resources available including intangibles such as personnel experience and skills, current programs and policies as well as tangibles including monies and budgets.

### 5.2.6 Security Management Assessment

The Security Management Assessment category asks what security policies are currently in effect, for example what policies are in effect for a bomb threat.

### 5.2.7 Critical Asset Assessment

The Critical Asset Assessment category is sub-divided into:

1. Electric Power
2. Telecommunications
3. Transportation
4. Support Services

Assets are “critical” when their loss either endangers human life or impacts the transit agency’s ability to maintain service. This step in the assessment process enables the agency to identify what assets must be protected, how these assets are valued both to the transit agency and a potential adversary as well as the impact if these assets are lost. Lost meaning to passengers, employees, public safety organization, general public and the transit operation. All assets are not critical, and some assets are only critical under certain conditions. This category asks the agency to list the assets that are mission critical. Without electric power, telecommunications, transportation and outside services available, it is necessary to have a contingency for redundancy in the system.\(^{22}\)

### 5.2.8 Threat and Vulnerability Assessment

The Threat and Vulnerability Assessment category follows directly after the critical asset inventory because it is important to identify and evaluate the vulnerabilities of these assets to specific threats,

\(^{22}\) Ohio Department of Transportation “Guide to Conducting Critical Asset Protection Self-Assessments”
and to promote reasoned decision-making which balances risk against the cost of protective countermeasures and enhanced emergency preparedness. This category asks the agency to look at historical data and identify “worst case scenarios” regarding security vulnerabilities.

### 5.2.9 Physical Security Systems Assessment

Physical Security Systems Assessment category asks the agency to evaluate the physical systems such as access authorization through badges, uniforms, barriers, perimeter controls as well as lock-down procedures. This category also has questions concerning the issuance of keys and if facilities are covered with closed-circuit-televisions.

### 5.2.10 Prevention Through Asset Hardening

Prevention through Asset Hardening asks the agency to identify the countermeasures, costs and tradeoffs for the prevention of an emergency by hardening the assets. On this phase of the activity it is important for the agency to focus on specific action items and recommendations to be implemented. The questions ask the agency to make design or operational changes to reduce risk levels by altering the nature of the asset such as additional procedural, technological or equipment measures that would reduce vulnerability. The Prevention category is sub-divided into:

1. Physical Control
2. Passenger Stations and Terminals
3. Control Center

**Physical Control**

The Physical Control category asks the agency if it is possible to install more security at critical points, institute tighter restrictions for visitors, perform structural hardening measures and perhaps implement vehicle-approach speed controls to name a few.

**Passenger Stations and Terminals**

The Passenger Stations and Terminals category asks the agency to take into consideration “hiding places” for explosive devices as well as securing or removing trash cans for possible threats.

**Control Center**

The Control Center category addresses the issues of creating a control center that that is secure from physical as well as virtual threats.

### 5.3 RESPONSE

Immediately following an event the response phase is initiated. Responding to an event involves mobilizing resources including emergency equipment, moving people away from danger, providing

---

23 Ibid
food, water, shelter, and medical services. States that are overwhelmed by a disaster make a request for federal aid, and the Federal Response Plan is implemented. Federal aid involves financial and the provision of resources, such as equipment and personnel. The Response category is sub-divided into:

1. Emergency Response Capabilities
2. Previous Experience
3. Response Training
4. Resources

5.3.1 Emergency Response Capabilities

Emergency Response Capabilities asks the agency what plans, policies, and procedures are in effect for an actual emergency. And more importantly do the employees, contractors, outside vendors know the emergency plan to act wisely if an does emergency take place.

5.3.2 Previous Experience

Previous Experience asks the agency to look at the last 12 months and evaluate the emergency response for its adequacy and efficiency. These questions are important to acknowledge if the agency was satisfied with its level of response and if not then where do the changes need to be made.

5.3.3 Response Training

Response Training outlines the specifics of the agency’s emergency response training program. For example, it is important to know if the equipment was available during a training program and if the coordination protocols were tested.

5.3.4 Resources

Resources category covers the redundancy factors such as the establishment of and Incident Command System and Command Post. It is recommended that the command post be situated a distance from the incident and ideally for an extended or sustained operation be located inside a building (a school, gymnasium, unoccupied store, or other similar site) or in a mobile command post facility such as a trailer, converted mobile home, or bus. There is also a question in this category to consider how to deal with the media during the crisis.

5.4 RECOVERY

Recovery is associated with the aftermath of the emergency and the next steps to restore normalcy. Rebuilding following an event can be the most challenging task of a disaster. Financial assistance is typically the largest element of recovery, through the Federal Response Plan capital resources are available to state and local agencies. Immediate recovery from a disaster involves developing employee tracking mechanisms, incident debriefings, and programs to help individuals manage stress associated with major disasters.

This category discusses tracking systems and debriefing mechanisms to understand how the emergency happened. Criminal investigations may play a role in the recovery process.
5.5 MITIGATION

Mitigation is key to emergency management. The goal is to reduce the impacts of disasters on individuals, agencies, and businesses. Mitigation involves the availability of redundant resources, equipment, and systems to enable a rapid response and recovery to normal operations. Proper mitigation planning includes multi-agency/stakeholder planning activities to identify needs and capabilities prior to an event. The questions in the Mitigation section cover the remediation and replacement of failed services as well as addresses the alternatives for loss of infrastructure and services.
6.0 NEEDS PRIORITIZATION PROCESS

This section will discuss various methods for prioritizing needs, identify a recommended methodology for need prioritization, and identify institutional issues likely to be associated with need prioritizations. This section follows from the previous section, the “Hybrid Self Assessment Tool”, by presenting methodologies with which to prioritize the needs that the organization identifies when it completes the questions contained in the Hybrid Tool.

6.1 QUANTITATIVE

The best quantitative method for prioritizing needs is the use of cost-benefit analysis (CBA). CBA is a systematic approach to the problem of choosing the best method of allocating scarce resources to achieve a given objective. A sound CBA recognizes that there are alternative ways to meet a given objective and that each alternative requires certain resources and produces certain results. To achieve a systematic evaluation, the CBA process employs the following two principles: Each feasible alternative for meeting an objective must be considered, and its life-cycle costs and benefits evaluated. The textbook steps for conducting a CBA include the following:

- Defining an objective or need;
- Identifying alternatives to achieve the objectives;
- Stating assumptions;
- Estimating the costs and benefits of each alternative and status quo; and
- Recommending a preferred alternative.

Defining an objective or need

The first step in a CBA is to define exactly what the problem is that the alternatives will attempt to solve. The problem might be that all of WMATA’s information technology (IT) systems have increased vulnerability (creating the need for improved IT security), or that a metro station or train is a target for a nuclear, chemical, or biological attack (creating the need for a nuclear, chemical, and biological detection sensor program), or that some emergency responders are unaware of how to respond to a WMATA emergency (creating the need for an emergency response training initiative). It is important that these problems and needs be tied to the organization’s mission or strategic objectives. Section 6.3 provides a framework for prioritizing needs against the Department of Homeland Security’s (DHS’s) strategic objectives.

Identifying alternatives to achieve the objectives

Once the problem or need is identified, the alternatives that will meet the problem or need should be identified. Alternatives are the different courses of action, means, or methods by which objectives can be obtained. It is important that the full range of alternatives are considered before beginning the analysis.
**Stating assumptions**

Once the alternatives to meeting the problem or need are identified, the next step is to develop a list of assumptions that can be used in the analysis. Documenting assumptions about the areas of the analysis that are straightforward and contain a lot of data is as important as documenting assumptions for those areas that are less clear. For those straightforward areas, it is good practice to provide a set of assumptions that provide every reader with the same common understanding. Assumptions like the number of years considered in the analysis, the systems covered with a proposed increased IT security system, or the agencies involved in the emergency response training initiative may seem obvious to the CBA team, but they will provide a common understanding to the audience. In addition, documenting assumptions for those areas of the analysis that are less clear is just as important. These are typically the assumptions that must be made so that the analysis can continue. Assumptions like the number of additional resources required to operate and maintain a proposed increased IT security system, how many sensors are required throughout the entire Metro system, or how long each training class is in the emergency response training program are important to get early consensus from as many people as possible. Finally, it is important to include assumptions that not only explain what is included in the analysis, but also what is **not** included.

**Estimating the costs and benefits of each alternative and status quo**

The development of costs and benefits for each alternative is the next step in a CBA. Identifying costs and benefits should be considered for all decisions that expend resources. There are various techniques that can be used to develop cost and benefit estimates, including:

- **Parametric:** to estimate the cost using a model that contains parameters that can be set based on the attributes of the project (e.g., software lines of code, project complexity, number of users, etc.).

- **Analogous:** to estimate the cost of an unknown item by comparing the unknown to a known item and its costs. This technique looks at observed or calculated values that are similar (e.g., size, functional area, scope, etc.).

- **Engineering:** to estimate the cost by estimating the costs of the system’s components and subcomponents and then summing up these costs.

- **Historical:** to estimate the cost by using past data (i.e., actuals) to estimate/forecast future data.

**Recommended a preferred alternative**

Once the costs and benefits have been identified for each alternative, the alternatives can be compared. There are various techniques that can be used to compare alternatives to assist decision-makers in choosing the right alternative, including:
• Net Present Value (NPV): adjusting each alternative’s stream of costs and benefits by using a discount rate\textsuperscript{24} that equates alternatives based on the “time value of money”.

• Return on Investment (ROI): using present value dollars to calculate how much of a return (i.e., benefit) a certain alternative will yield on an investment (i.e., cost).

• Break-even point/payback: determining how many years it will take for a certain alternative’s cumulative benefits to surpass the cumulative costs.

\section*{6.2 QUALITATIVE}

Qualitative methodologies use expert assessment and relative ranking scales to identify measures for costs and benefits associated with security issues and projects and guide investments within available resources. They also provide relative prioritization of security risks and identify areas for improvement against vulnerabilities.\textsuperscript{25} The qualitative methodologies are often supported by checklists, templates and other guides to direct execution.

Qualitative methodologies rely on ordinal probabilities and consequences, assigned based on expert judgment in terms such as: certain, high, medium, low, rare, very rare, catastrophic, critical, major, minor, minimal and none.

As mentioned in Section 1.1, the Homeland Security Act of 2002 mandates that the National Capital Region, among others, must submit an annual report to Congress that includes the following:

1. The identification of the resources required to fully implement homeland security efforts in the National Capital Region;

2. An assessment of the progress made by the National Capital Region in implementing homeland security efforts; and

3. Recommendations to Congress regarding the additional resources needed to fully implement homeland security efforts in the National Capital Region.

Since DHS is less than a year old, most of its policies and procedures are either relatively immature or have not yet been produced. Therefore, it is unclear exactly how the department will evaluate projects against each other, much less against the measure of “homeland security efforts” that is cited above. A review of DHS’s “National Strategy for Homeland Security” however, provides insight into the department’s vision and its strategic objectives. As this document states, it “establishes a foundation upon which to organize [the department’s] efforts and provides initial guidance to prioritize the work ahead.”


National Strategy for Homeland Security

The National Strategy for Homeland Security categorizes homeland security functions into the following six “critical mission areas”:

- intelligence and warning,
- border and transportation security,
- domestic counter terrorism,
- protecting critical infrastructure,
- defending against catastrophic terrorism, and
- emergency preparedness and response.

Each of these “critical mission areas” contains “major initiatives” that are specific to each area. Although each area contains between 5 to 12 “major initiatives”, most of the initiatives do not relate to WMATA’s transportation mission. These initiatives have been removed from the prioritization analysis described in this section, leaving 14 WMATA-relevant DHS initiatives. These 14 are listed below, associated with their “critical mission area”.

Domestic Counterterrorism

- Improve intergovernmental law enforcement coordination
- Facilitate apprehension of potential terrorists
- Continue ongoing investigations and prosecutions

Protecting Critical Infrastructure and Key Assets

- Enable effective partnership with state and local governments and the private sector
- Harness the best analytic and modeling tools to develop effective protective solutions
- Guard America’s critical infrastructure and key assets against "inside" threats

Defending Against Catastrophic Threats

- Prevent terrorist use of nuclear weapons through better sensors and procedures
- Detect chemical and biological materials and attacks
- Improve chemical sensors and decontamination techniques

WMATA is encouraged to review the complete list of major initiatives to determine if the study group overlooked any that are, in fact, relevant to WMATA.
- Harness the scientific knowledge and tools to counter terrorism

**Emergency Preparedness and Response**

- Improve tactical counterterrorist capabilities
- Enable seamless communication among all responders
- Prepare health care providers for catastrophic terrorism
- Prepare for chemical, biological, radiological, and nuclear decontamination

These 14 WMATA-relevant DHS initiatives will be used in Section 6.2.2 to illustrate a methodology for prioritizing WMATA’s projects and initiatives in support of DHS’s efforts.

**Goals of Prioritization**

The National Strategy for Homeland Security states that “decisions on homeland security activities and spending must achieve two overarching goals: to devote the right amount of scarce resources to homeland security and to spend these resources on the right activities.” This process of prioritization, and the methodology prescribed in this chapter, focuses on the second goal. The National Strategy describes this goal by explaining that “because some activities might achieve substantial benefits at low cost, while others result in minimal gain at a high price, resources should be shifted to their most ‘productive’ use.” While Section 6.1 described the use of measures like Return On Investment (ROI), Cost-Benefit Ratios (CBRs), and Net Present Value (NPV), there is another way to analyze projects and initiatives against an organization’s goals by using a process called a Goals Achievement Methodology.

### 6.2.1 Goals Achievement Methodology

The Goals Achievement Methodology enables competing projects to be compared against each other by using an established set of criteria. Commonly used criteria consist of features like lives saved, reduction in travel time, mean time between failure, mean time to repair, and even the quantitative measures described in Section 6.1 (e.g., ROI, CBRs, and NPV). A more useful application of this methodology, however, is to compare projects against the organization’s goals, and to evaluate each project’s ability to impact those goals. The next few sections describe this approach and provide some sample data to illustrate how this approach is used.

**Goals Achievement Methodology Template**

This section describes the goals achievement template that has been prepared for WMATA using the National Strategy for Homeland Security’s “critical mission areas” and “major initiatives” as evaluation criteria. Table 6.1 illustrates the “critical mission areas” and “major initiatives” along the left and placeholders for WMATA’s projects and initiatives across the top.
## Table 6.1 Goals Achievement Methodology Template

<table>
<thead>
<tr>
<th>&quot;Critical Mission Areas&quot; and &quot;Major Initiatives&quot;</th>
<th>WMATA Projects / Initiatives</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CMA #3: Domestic Counterterrorism</strong></td>
<td>Weighting</td>
</tr>
<tr>
<td>Improve intergovernmental law enforcement</td>
<td>Project 1</td>
</tr>
<tr>
<td>coordination</td>
<td>Project 2</td>
</tr>
<tr>
<td>Facilitate apprehension of potential terrorists</td>
<td>Project 3</td>
</tr>
<tr>
<td>Continue ongoing investigations and prosecutions</td>
<td>Project N</td>
</tr>
<tr>
<td><strong>CMA #4: Protecting Critical Infrastructure and Key Assets</strong></td>
<td>To be determined</td>
</tr>
<tr>
<td>Enable effective partnership with state and</td>
<td></td>
</tr>
<tr>
<td>local governments and the private sector</td>
<td></td>
</tr>
<tr>
<td>Harness the best analytic and modeling tools</td>
<td></td>
</tr>
<tr>
<td>to develop effective protective solutions</td>
<td></td>
</tr>
<tr>
<td>Guard America’s critical infrastructure and</td>
<td></td>
</tr>
<tr>
<td>key assets against &quot;inside&quot; threats</td>
<td></td>
</tr>
<tr>
<td><strong>CMA #5: Defending Against Catastrophic Threats</strong></td>
<td></td>
</tr>
<tr>
<td>Prevent terrorist use of nuclear weapons</td>
<td></td>
</tr>
<tr>
<td>through better sensors and procedures</td>
<td></td>
</tr>
<tr>
<td>Detect chemical and biological materials and</td>
<td></td>
</tr>
<tr>
<td>attacks</td>
<td></td>
</tr>
<tr>
<td>Improve chemical sensors and decontamination</td>
<td></td>
</tr>
<tr>
<td>techniques</td>
<td></td>
</tr>
<tr>
<td>Harness the scientific knowledge and tools to</td>
<td></td>
</tr>
<tr>
<td>counter terrorism</td>
<td></td>
</tr>
<tr>
<td><strong>CMA #6: Emergency Preparedness and Response</strong></td>
<td></td>
</tr>
<tr>
<td>Improve tactical counterterrorist capabilities</td>
<td></td>
</tr>
<tr>
<td>Enable seamless communication among all</td>
<td></td>
</tr>
<tr>
<td>responders</td>
<td></td>
</tr>
<tr>
<td>Prepare health care providers for</td>
<td></td>
</tr>
<tr>
<td>catastrophic terrorism</td>
<td></td>
</tr>
<tr>
<td>Prepare for chemical, biological, radiological,</td>
<td></td>
</tr>
<tr>
<td>and nuclear decontamination</td>
<td></td>
</tr>
</tbody>
</table>

---

**Key areas** identified in the President’s Budget for FY03 *for extra attention and carefully targeted increases in federal expenditures*

**It is expected that in FY04 the Administration will attach priority to the following items**
The President’s Budget for Fiscal Year 2003 identified the following four key areas for extra attention and carefully targeted increases in federal expenditures:

- Support first responders.
- Defend against biological terrorism.
- Secure America’s borders.
- Use information to secure the homeland.

In addition, it is expected that the President’s Budget for Fiscal Year 2004 will attach priority to the following items:

- Enhance the analytic capabilities of the FBI
- Build new capabilities through the Information Analysis and Infrastructure Protection Division of the proposed Department of Homeland Security
- Create “smart borders”
- Increase the security of international shipping containers
- Recapitalize the U.S. Coast Guard
- Prevent terrorist use of nuclear weapons through better sensors and procedures
- Develop broad spectrum vaccines, antimicrobials, and antidotes
- Integrate information sharing across the federal government”

The four shaded areas in Table 6.1 represent the “major initiatives” that relate to the priorities identified in the President’s Budget. The light blue-shaded area represents the one “major initiative” that relates to the President’s Budget for Fiscal Year 2003; the tan-shaded areas represents the “major initiatives” that relate to the President’s Budget for Fiscal Year 2004.
**Goals Achievement Methodology Sample**

This section uses the goals achievement template from the previous section and populates the matrix with sample data that might represent the scoring for three sample projects or initiatives. One approach to scoring the projects is to have each project or initiative score their own, but a better approach is to have a group of representative individuals, who have no immediate vested interest, complete the scoring by comparing the projects against each other. Although the scoring is somewhat arbitrary (i.e., a “5” does not have a direct meaning in and of itself), the importance is scoring the projects relative to the other projects (i.e., a project that receives a “7” is slightly better than a project that receives a “5” against the same “major initiative”).

Table 6.2 illustrates the matrix with completed scores for three projects labeled “Project 1”, “Project 2”, and “Project 3”.

<table>
<thead>
<tr>
<th>&quot;Critical Mission Areas&quot; and &quot;Major Initiatives&quot;</th>
<th>WMATA Projects / Initiatives</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMA #3: Domestic Counterterrorism</td>
<td>Weighting</td>
</tr>
<tr>
<td>Improve intergovernmental law enforcement coordination</td>
<td>1</td>
</tr>
<tr>
<td>Facilitate apprehension of potential terrorists</td>
<td>1</td>
</tr>
<tr>
<td>Continue ongoing investigations and prosecutions</td>
<td>1</td>
</tr>
<tr>
<td>CMA #4: Protecting Critical Infrastructure and Key Assets</td>
<td></td>
</tr>
<tr>
<td>Enable effective partnership with state and local governments and the private sector</td>
<td>1</td>
</tr>
<tr>
<td>Harness the best analytic and modeling tools to develop effective protective solutions</td>
<td>1</td>
</tr>
<tr>
<td>Guard America's critical infrastructure and key assets against &quot;inside&quot; threats</td>
<td>1</td>
</tr>
<tr>
<td>CMA #5: Defending Against Catastrophic Threats</td>
<td></td>
</tr>
<tr>
<td>Prevent terrorist use of nuclear weapons through better sensors and procedures</td>
<td>3</td>
</tr>
<tr>
<td>Detect chemical and biological materials and attacks</td>
<td>2</td>
</tr>
<tr>
<td>Improve chemical sensors and decontamination techniques</td>
<td>1</td>
</tr>
<tr>
<td>Harness the scientific knowledge and tools to counter terrorism</td>
<td>1</td>
</tr>
<tr>
<td>CMA #6: Emergency Preparedness and Response</td>
<td></td>
</tr>
<tr>
<td>Improve tactical counterterrorist capabilities</td>
<td>1</td>
</tr>
<tr>
<td>Enable seamless communication among all responders</td>
<td>2</td>
</tr>
<tr>
<td>Prepare health care providers for catastrophic terrorism</td>
<td>1</td>
</tr>
<tr>
<td>Prepare for chemical, biological, radiological, and nuclear decontamination</td>
<td>2</td>
</tr>
</tbody>
</table>

---

"Key areas" identified in the President's Budget for FY03 "for extra attention and carefully targeted increases in federal expenditures"

"It is expected that in FY04 the Administration will attach priority to the following items"
In Table 6.2, sample weightings are provided to help differentiate between the value of each DHS “major initiative”. Weightings are an important, although subjective, aspect, as they enable each “major initiative” to be distinguished from the others based on importance to the organization. In Table 6.2, the key areas from the President’s FY03 budget have been assigned a weight twice that of the “major initiatives” that were not highlighted in the FY03 budget. Likewise, the aspects given priority in the President’s FY04 budget have been assigned a weight three times that of the “major initiatives” that were not highlighted in the FY03 budget. It is important to note that no analysis has been conducted to determine these weightings; the study team is using these weights for illustrative purposes only. Representatives within the impacted organizations should determine the appropriate weightings.

In Table 6.2, “Project 1” represents improved information technology (IT) security, which explains the higher scoring for the communication and collaboration aspects, and the lower scoring for the nuclear and chemical detection aspects. “Project 2” represents a sensor program, which explains the higher scoring for the nuclear and chemical detection aspects, and the lower scoring for the communication and collaboration aspects. “Project 3” represents an emergency response training initiative, which explains the higher scoring for the preparedness aspects, and the lower scoring for the nuclear and chemical detection aspects.

**Goals Achievement Methodology Sample Results**

This section uses the sample data and weightings from the previous section and computes each project’s result when its score is multiplied by the respective weighting. For the DHS “major initiatives” where the weighting was a “1”, the scores from Table 6.2 have been carried forward as the resultant score. However, when the DHS “major initiatives” were weighted with a “2” or a “3”, the scores from Table 6.2 have been multiplied by a “2” or a “3”, respectively, which doubles or triples the importance of scoring higher against those “major initiatives”.

Table 6.3 illustrates the matrix with the resultant scores for the three projects labeled “Project 1”, “Project 2”, and “Project 3”.
Table 6.3 Goals Achievement Methodology Sample Results

<table>
<thead>
<tr>
<th>&quot;Critical Mission Areas&quot; and &quot;Major Initiatives&quot;</th>
<th>Weighting</th>
<th>Project 1</th>
<th>Project 2</th>
<th>Project 3</th>
<th>...</th>
<th>Project N</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CMA #3: Domestic Counterterrorism</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Improve intergovernmental law enforcement coordination</td>
<td>1</td>
<td>7</td>
<td>6</td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Facilitate apprehension of potential terrorists</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Continue ongoing investigations and prosecutions</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>CMA #4: Protecting Critical Infrastructure and Key Assets</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable effective partnership with state and local governments and the private sector</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Harness the best analytic and modeling tools to develop effective protective solutions</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Guard America’s critical infrastructure and key assets against “inside” threats</td>
<td>1</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>CMA #5: Defending Against Catastrophic Threats</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prevent terrorist use of nuclear weapons through better sensors and procedures</td>
<td>3</td>
<td>0</td>
<td>30</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Detect chemical and biological materials and attacks</td>
<td>2</td>
<td>10</td>
<td>20</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Improve chemical sensors and decontamination techniques</td>
<td>1</td>
<td>0</td>
<td>10</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Harness the scientific knowledge and tools to counter terrorism</td>
<td>1</td>
<td>4</td>
<td>7</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>CMA #6: Emergency Preparedness and Response</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Improve tactical counterterrorist capabilities</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable seamless communication among all responders</td>
<td>2</td>
<td>18</td>
<td>0</td>
<td>10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prepare health care providers for catastrophic terrorism</td>
<td>1</td>
<td>3</td>
<td>4</td>
<td>10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prepare for chemical, biological, radiological, and nuclear decontamination</td>
<td>2</td>
<td>6</td>
<td>10</td>
<td>16</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Totals</td>
<td>59</td>
<td>97</td>
<td>67</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

As can be seen in Table 6.3, “Project 2”, the sensor program, with its high scores in the nuclear and chemical detection categories, offsets its poor scores in some of the other categories. Based on the scoring and the weightings used, this project finishes with a total of 97 points. It is important to note, however, that these scores and, consequently, the order of the projects, are heavily impacted by the weighting assigned. Care must be given to the weightings that are applied to each DHS initiative.

6.2.2 Security Risk Index Methodology

The Security Risk Index Methodology (SRI) is another example of a qualitative methodology to rank WMATA facilities in terms of importance. This method helps to analyze various facilities and assets in order to prioritize them against each other and creating an higher index that would indicate which facility should be ranked high against other facilities competing for the same resources. For example, facilities like Metro Center may rank higher because of the complexity of infrastructure, importance of the buildings in the area, and the number of people using the facility. However, the Vienna station may rank low since it has two tracks and fewer number of users. As a result, if Vienna is closed and operations stop due to an attack or bomb threat, the movement of people would not be affected as much. Thus, available resources should be directed to Metro Center first and Vienna last.

The SRI has three areas of concern: Difficulty of Attack, Severity of Attack, and Attractiveness of Target. The following three tables describe each of these areas in detail. The difficulty of attack takes into account such factors as the level of security at the facility (individuals or specialized equipment in operation etc). The focus is on the layers of security that one has to breach to reach the target. Severity of attack is estimated based upon the population at the facility within a certain radius of the
facility. Attractiveness of target is estimated based on factors such as potential disruption to the local or national economy or infrastructure and the likely level of public concern. Table 6.4 describes the factors which influence the Difficulty of Attack. Table 6.5 focuses on the Severity of Attack and the complexity of WMATA facilities and the number of people using that facility. Table 6.6 indicates the attractiveness of the target and provides a description and factors that will influence the attractiveness of target to attack.

**Table 6.4 Relative Difficulty of Attack**

<table>
<thead>
<tr>
<th>DESCRIPTION OF FACTORS WHICH INFLUENCE THE LIKELIHOOD OF ATTACK</th>
<th>EXAMPLES</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 The scenario could be caused by a successful attack, which would require a well-planned and coordinated series of events involving several individuals with special knowledge /training and breaching several independent security levels of protection</td>
<td>Hijacking of commercial aircraft; organized paramilitary attack within a facility</td>
</tr>
<tr>
<td>2 The scenario could be caused by a successful attack, which could be accomplished by a small group of individuals with equipment or materials available to organized terrorist organizations (or insider with special knowledge of the facility), and does require access to restricted access areas</td>
<td>Use of explosive materials within the facility boundaries; use of control system to override protective layers via access to control system.</td>
</tr>
<tr>
<td>3 The scenario could be caused by a successful attack, which could be accomplished by a small group of individuals with equipment or materials available to organized terrorist organizations, but does not require access to restricted access areas.</td>
<td>Use of explosive materials from outside the plant boundaries; disgruntled employee with access to small size explosives</td>
</tr>
<tr>
<td>4 The scenario could be caused a successful attack accomplished by a single individual with readily available equipment.</td>
<td>A bomb blast inside a facility</td>
</tr>
</tbody>
</table>

**Table 6.5 Relative Severity of Attack**

<table>
<thead>
<tr>
<th>SEVERITY OF ATTACK WILL BE BASED ON COMPLEXITY OF INFRASTRUCTURE AND VOLUME OF PASSENGERS</th>
<th>BOMB BLAST SCENARIO</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 2 tracks with 1000 passengers per day</td>
<td></td>
</tr>
<tr>
<td>2 2 tracks with 1000 to 10, 000 passengers per day</td>
<td></td>
</tr>
<tr>
<td>3 2 tracks with 10,000 to 100, 000 per day</td>
<td></td>
</tr>
<tr>
<td>4 4 tracks with 100, 000 or greater</td>
<td></td>
</tr>
</tbody>
</table>

---

Table 6.6  Attractiveness of Target

<table>
<thead>
<tr>
<th>DESCRIPTION AND FACTORS WHICH INFLUENCE THE ATTRACTIVENESS OF TARGET TO TERRORISTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
</tr>
<tr>
<td>A successful attack is unlikely to cause disruption to local economy or local infrastructure. Therefore an attack is unlikely to create more than limited localized attention.</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>A successful attack could cause local evacuations, disruption to local economy or disruption of local infrastructure. Such attack would cause primary local concern and attention.</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>A successful attack could impact regional economy, disruption of regional infrastructure, or cause extensive property damage. Such an attack would be likely to generate some national concern and attention.</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>Facility located adjacent to a major recognizable landmark such as Washington DC or New York City. A successful attack could impact national economy, disrupt a major supply of a critical material or national infrastructure. Such an attack would create significant national / international concern and attention.</td>
</tr>
</tbody>
</table>

In order to utilize SRI method, WMATA will have to identify and analyze various assets/facilities that will compete for the limited available resources and calculate the Security Risk Index. Below are four examples of using the SRI method to analyze four WMATA Metrorail stations: Metro Center, Pentagon, Ronald Regan National Airport and Vienna. The Security Risk Index will determine the priority that should be given to the facility and enable WMATA to better prioritize available resources.

In completing this task, each facility is analyzed against the three areas of concern mentioned above: difficulty of attack, severity of attack and attractiveness of target. For each of the three areas, the facility is ranked on a scale of 1 – 4. This results in each facility receiving a score between 3 to 12. A facility with a score of 1 in difficulty of attack, 1 in severity of attack and another 1 on attractiveness of target will receive a total score of 3 (see Table: 6.7 Vienna Metro Station SRI) and will rank low in the needs prioritization list. On the other hand a facility that has a score of 4 in difficulty of attack, a 4 on severity of attack and a 4 on attractiveness of target will receive a total score of 12 (see Table 6.4: Metro Center Station SRI) and this would place it higher in the list of needs prioritization.

The tables below indicate how the security index can be calculated and employed to prioritize the needs of an agency. This prioritization tool was designed by American Chemistry Council after 9/11 to determine which facilities needs to be attended to first in terms of security, and also used the tool to see if its tier 4 facilities can be upgraded to the next tier. The examples given below helps to clarify how the tool can be employed to meet the needs of WMATA. The following WMATA facilities have been selected to demonstrate how the security index is calculated:- Metro station, Ronald Reagan National Airport, Vienna and Pentagon City.
Metro Center Station

Table 6.7 Metro Center Station SRI

<table>
<thead>
<tr>
<th>DIFFICULTY OF ATTACK</th>
<th>SEVERITY OF ATTACK</th>
<th>ATTRACTIVENESS OF TARGET</th>
<th>SECURITY RISK INDEX (SRI)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td>4+3+4=11</td>
</tr>
</tbody>
</table>

The Metro Center SRI is calculated as 11 since there are two tracks in the lower level and two tracks in the upper level, this facility is used by a large number of the people, the fact that it is a public facility with no security facilities for scanning and/or detecting dangerous weapons and substances makes the facility to be a priority. In addition disruption of this facility would affect movement of people in DC, and Virginia and would result in a national concern.

Pentagon Station

Table 6.8 Pentagon Station SRI

<table>
<thead>
<tr>
<th>DIFFICILTY OF ATTACK</th>
<th>SEVERITY OF ATTACK</th>
<th>ATTRACTIVENESS OF TARGET</th>
<th>SECURITY RISK INDEX (SRI)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td>3+3+4=10</td>
</tr>
</tbody>
</table>

Pentagon ranks high also because this facility is used by a large number of people, it has facilities for buses as well. Above all the area has important buildings like the Pentagon. As a result, any harm with a high impact will have a significant national and international concern.

Ronald Regan National Airport Station

Table 6.9 Ronald Regan Nation Airport Station SRI

<table>
<thead>
<tr>
<th>DIFFICILTY OF ATTACK</th>
<th>SEVERITY OF ATTACK</th>
<th>ATTRACTIVENESS OF TARGET</th>
<th>SECURITY RISK INDEX (SRI)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td>2+1+3=6</td>
</tr>
</tbody>
</table>

Ronald Reagan National Metro Station is in the middle because few people use it and it is mainly used by Air travelers. These people have to go through airport security checks, so the level of threat
is minimal. The disruption of the facility will not cause a major problem in the transportation network of the region.

**Vienna Station**

Table 6.10 Vienna Station SRI

<table>
<thead>
<tr>
<th></th>
<th>DIFFICLTY OF ATTACK</th>
<th>SEVERITY OF ATTACK</th>
<th>ATTRACTIVENESS OF TARGET</th>
<th>SECURITY RISK INDEX (SRI)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td>1+1+1=3</td>
</tr>
</tbody>
</table>

Vienna though used by a sizeable number of the population is ranked low on the grounds that the location is not that attractive.

The above-mentioned facilities have been ranked according to their importance, the rankings indicate that facilities such as the Pentagon and Metro Center would be slotted into the Tier 1 category due to their importance to the regional economy while Reagan and Vienna rank low because they are less important when set side by side with facilities slotted in the Tier 1 category.

Table 6.11 SRI Tier Index

<table>
<thead>
<tr>
<th>SECURITY RISK INDEX</th>
</tr>
</thead>
<tbody>
<tr>
<td>TIER 4</td>
</tr>
<tr>
<td>3 Vienna</td>
</tr>
</tbody>
</table>

6.3 BASELINE METHODOLOGY

Baseline methodologies categorize facilities and systems by types and assign specific allocations based on pre-determined criteria. “The organization which takes a baseline approach has already integrated anti-terrorism measures into its design criteria and operating procedures, and simply requires the analysts to determine which criteria and / or procedures are appropriate for a given site or facility. MCCormic:2003)” Prioritization can be executed by ranking facilities according to importance using some of the parameters outlined by GSA. The General Services Administration’s (GSA) five level classification system, include parameters such as occupancy, size, level of public contact, type of operations, and the nature of agencies present in the facility. As a result, some of
the items listed in the classification can be tailored to be agency specific. The GSA Classification System is:28

- **Level V**: Buildings with mission functions critical to national security (e.g., Pentagon and CIA Headquarters in Langley, VA).

- **Level IV**: Buildings with 451 or more federal employees, high level of contact with the public, more than 150,000 sq feet of space, and high-risk tenant agencies with highly sensitive records.

- **Level III**: Buildings with 151 to 450 federal employees, moderate to high level of contact with the public, 80,000 square to 150,000 square feet of space, and high-risk tenant agencies with highly sensitive records.

- **Level II**: Buildings with 11 to 150 Federal employees, moderate levels of public contact, 2,500 to 80,000 square feet of space, and tenants that have routine missions.

- **Level I**: Buildings with 10 or fewer federal employees, low levels of public contact with only a small segment of the population, and 2,500 square feet of space or less.

The table below ranks WMATA facilities according to GSA classification. The facilities ranked are as follows: control center, guideways, tunnels, vehicles, stations, Storage (parking facilities) would be ranked according to the level of importance.

---

28 General Services Administration’s Classification (Source: MCCORMICK, TAYLOR RESEARCH TEAM: Summary of resources prioritizing transportation anti-terrorism security measures, 2003)
### Table 6.12 WMATA Facilities and GSA Classification System

<table>
<thead>
<tr>
<th>FACILITY</th>
<th>LEVEL I</th>
<th>LEVEL II</th>
<th>LEVEL III</th>
<th>LEVEL IV</th>
<th>LEVEL V</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Center</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vehicles</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Guideways</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tunnels</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tunnels (with buildings and functions critical to national security)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In the above example, facilities such as the control center and tunnels with buildings with functions critical to national security such as the Pentagon have been given higher rankings. The disruption of the control center would adversely affect transportation in the region, while an attack on the storage facilities would lead to the vehicles being destroyed thus hampering smooth transportation of people in the region.

The methodologies presented above, consisting of the quantitative, qualitative, and baseline approaches, will provide WMATA with a method of prioritizing its needs in order to accommodate competing interests and limited resources. These methodologies can also be used by oversight organizations (e.g., DHS, the Office for National Capital Region Coordination) to make these same prioritization decisions across all departments, bureaus, and agencies within its organization.
7.0 FINDINGS AND RECOMMENDATIONS

The goal of this report was to develop a product designed to assist WMATA in conducting a self-assessment of its infrastructure security required for the National Capital Region by the Homeland Security Act of 2002. Additionally, it provides recommended prioritization methodologies to assist WMATA in allocating time and resources to security related improvements at the regional level. To complement the Regional Emergency Coordination Plan (RECP) and the FTA's WMATA vulnerability assessment, this report also describes various tools available today of the scope and type most useful for WMATA's needs.

The RECP was designed to allow regional governments in the National Capital Region to effectively plan, communicate, coordinate, and share information during actual emergencies. As described, the RECP is comprised of the Regional Incident Communication and Coordination System (RICCS), Regional Emergency Support Functions (R-ESFs), and associated annexes, all of which provide the coordination framework needed during such an emergency.

WMATA has one of the most complex tasks for vulnerability assessment as it operates rail and bus services in the majority of the COG jurisdictions. Through this vast region, it must coordinate with 18 separate governments located throughout Northern Virginia, Maryland, and the District of Columbia ensuring the same level of coordination takes place throughout the region regardless of jurisdiction. For example, WMATA must make certain the response to a potential incident in Montgomery Co. Maryland must be as planned and coordinated as one in Arlington Co. Virginia. Guaranteeing that type of seamless coordination is a daunting task.

One of the recommended methods WMATA can use to comply with Homeland Security Act of 2002's intent and plan cohesive responses across those many jurisdictions is the use of a self-assessment tool. As described in Chapter 4, there are multiple tools available and in use to evaluate infrastructure security and recommend corrective action when needed, but none are specifically designed to address compliance with the Homeland Security Act. After assessing the attributes of the 15 tools selected for review, the WashCOGs RECP scored in the highest category, "robust", for addressing all four response phases and attaining at least 15 "high" marks in addressing evaluation criteria.

Although all of the 15 tools reviewed have individual merit, none comprehensively fit WMATA's particular need. This led to the development of the Hybrid Tool described in Chapter 5. This hybrid was developed specifically for the critical infrastructure needs and assessments in the National Capital Region. The tool is designed in a checklist format for ease of use and is broken out by five categories (Planning & Prevention, Response, Recovery, and Mitigation). Each of the questions listed under these categories was specifically selected and tailored to address WMATA's needs. This tool, in conjunction with the RECP, will take WMATA through the necessary steps towards compliance with the requirements of the Homeland Security Act of 2002.

Once WMATA defines its specific needs for compliance with the Homeland Security Act of 2002, prioritization is critical to efficiently utilize the limited resources for the greatest good. Chapter 6 discusses the various quantitative and qualitative methods recommended for use in needs prioritization such as Cost Benefit Analysis (CBA), Goals Achievement Methodology, and Security Risk Index Methodology. The Goals Achievement Methodology is the recommended approach as it
provides the foundation for evaluating projects against the actual critical mission areas and major initiatives identified in the National Strategy for Homeland Security.

A two pronged approach is recommended to address WMATA's infrastructure security and vulnerability self-assessment. Although the Model/Framework tools are perhaps the best choice of the available assessment tools, they are time and resource intensive requiring great effort upon the organizations for use. The best solution would be to use the Hybrid Tool as a starting point to ensure that all possible areas of concern have been identified. Initial work on solutions can begin immediately and any critical shortfalls identified can be addressed in short order. As time and resources become available, we do recommend the implementation of a Model/Framework designed tool such as the RECP. It is more comprehensive in nature than the questionnaire and will give a greater detailed and specific map of tasks to be accomplished in order to satisfy the mandated Homeland Security Act of 2002 and Congressional requirements.

Even if all shortfalls and requirements are identified, without prioritization the critical issues may not get the appropriate attention. Again, a two-pronged approach to solving prioritization issues is suggested. The Goals Achievement Methodology is the recommended approach as it provides the foundation for evaluating projects against the actual critical mission areas and major initiatives identified in the National Strategy for Homeland Security. This, in conjunction with the Hybrid self-assessment tool, will give WMATA's leadership a good initial road map of critical needs.
Appendix A: Self-Assessment Tool Summaries
ASSESSING EMERGENCY PREPAREDNESS OF TRANSIT AGENCIES: A FOCUS ON PERFORMANCE INDICATORS

The focus of this paper is on emergency preparedness of transit agencies and a method in which preparedness can be assessed and systematically monitored using performance indicators. Performance indicators can play a very important role in the systematic monitoring of the emergency preparedness of transit agencies. Firstly, performance indicators can act as an assessment tool to determine how well the goals of a transit agency are being met. Secondly, performance indicators can be used to identify problems and motivate managers and staff. Thirdly, performance indicators assessing a transit agency’s level of preparedness must reflect elements that contribute to the success of an emergency response effort and should arise out of the objectives and policies developed in the agency’s emergency preparedness plan.

Transit agencies should cooperate with other agencies to assess their region’s vulnerabilities to incidents of various types. Assessment should identify susceptible areas and degrees of vulnerability for each type of risk. The agency should establish its emergency management policies and goals ensuring they are compatible with regional ones. Transit agency should then perform an emergency response capability assessment by inventorying available fleet and operating staff and share its assessment with other agencies. The agency’s policies and goals and the plan should coincide with the multi-agency’s area wide plan and should be developed in consultation with other pertinent agencies. A good preparedness plan will incorporate the results of available simulation models, drill, or actual incident.

The four categories of indicators discussed in this paper include fleet management and control, communications and coordination, traveler information and training.

FLEET MANAGEMENT

During emergencies, bus fleet management and control are essential especially for agencies with large fleets. As a result the following should be taken into account:

- Percentage of fleet equipped with functioning AVL and control equipment
- Percentage of service area reliability covered by the vehicle tracking equipment
- Percentage of signals in service area with transit priority
- Existence of chain of command and communications protocol
- Existence of contingency plan a) in case of total systems failure b) to ensure continuation of transportation services to vital facilities

COMMUNICATIONS AND COORDINATION

A pre-determined communications procedure and chain of command protocol will minimize confusion during emergency response efforts. This must occur on two levels intra-agency and inter-agency. Communications equipment should be functioning at all times and presence of backup
systems in the event of IT systems failure. In order to ensure that the objectives of this plan the following should be noted:

- Percentage of functioning primary communications systems within transit facilities and in service area
- Percentage of key personnel who have access to the communications system
- Percentage of functioning secondary or backup communications systems within transit facilities and in service area.
- Existence of backup systems in the event of IT systems failure
- Existence of a hotline or similar device to facilitate simultaneous communication with other pertinent response agencies
- Degree of intra-agency and inter-agency information sharing
- Demonstrable knowledge of intra-agency and inter-agency chain of command and communications procedures via test or drills.
- Access to primary and secondary systems by all key personnel

**TRAVELER INFORMATION**

- Number of methods used to disseminate real time transit information to the public
- Accuracy of information provided to the public
- Reliability of the information delivery method
- The frequency of information updates

**TRAINING**

- Percentage of key transit personnel and operating personnel that undergo training
- Comprehensiveness of training program
- Level of real world experience derived by participants
- Frequency of refresher training
- Percentage correct responses in an exam /simulation / drill.

The performance indicators will identify an agency’s weaknesses and possible areas of improvement. Transit agencies should then identify alternatives to address the vulnerabilities highlighted by the performance indicators and perform a comprehensive cost-benefit analysis to select the optimal alternative.
COMMUNICATION OF THREATS: A GUIDE (TCRP REPORT 86)

The Transit Cooperative Research Program’s (TCRP’s) “Communication of Threats: A Guide” states that it:

“…offers information on a variety of approaches to improving the sharing of threat information. Current practices, operational needs, technologies for threat information dissemination, and system functional requirements are discussed. Effective strategies for sharing analyzed and unanalyzed reports of suspicious activities and a path to an interoperable set of national, regional, and local threat-information forums are proposed.”

However, as the scoring indicates (on the criteria/rating matrix), this guide barely skims the surface of vulnerability issues. The first major section of the guide offers the results of a survey that was generated and distributed to 39 public transportation systems to determine the current sources of threat information they receive. The first half of the guide is devoted to describing the survey and listing the survey questions (e.g., what are desirable attributes of a threat communication system?, what level of security is required?) and the second half of the guide discusses the technologies that are available to create a threat dissemination system. Although this latter half is valuable to the creation of software solution to the lack of threat information sharing, the guide does not prove useful to our efforts.
EMERGENCY PREPAREDNESS FOR TRANSIT TERRORISM (TCRP SYNTHESIS 27)

The TCRP-27 synthesizes information from surveys, literature review, interviews and onsite visits of transit agencies to outline current practice of planning and response activities to terrorist acts. The document also looks at the history and extent of terrorism related to transit agencies as well as emerging threats. The paper takes considers each area of emergency management (planning, response, recovery, and mitigation) with an emphasis on planning and response activities.

The theme of the paper is toward an increased responsibility of transit agencies for terrorism preparedness and response and emphasizes interagency as well as interagency cooperation. Although not an assessment tool per se, TCRP 27 outlines specific emergency preparedness and response planning and mitigation activities that likely should be addressed in any assessment tool for transit operations. The document also outlines important aspects of the other phases of emergency management i.e. response and recovery.

The consideration of the recommendations in this document would aid in the assessment of a transit agency’s overall preparedness for terrorist actions.

PLANNING

The document discusses planning aspects related to mitigating and responding to terrorism, emphasizing ways to improve Intragency, interagency as well as inter-jurisdictional cooperation.

INTRAGENCY

Considers management issues related to the designation of authority and the commitment of resources to develop plans and procedures. Planning exercises such as the formation of a terrorism preparedness-planning group or the required development of the System Security Program Plan (SSPP) aids in identifying intra-agency responsibilities and to examine and strengthen both intra-agency and inter-agency relationships.

INTER-AGENCY AND INTER-JURISDICTIONAL

Improve inter-agency (local, state, and federal law enforcement and emergency services) relationships (considered in the SSPP). Specific points include transit agency access to crime data and intelligence analysis, as well as defining the jurisdictional roles of various agencies.

MITIGATION

The document outlines important aspects involved in the risk assessment and (and threat) analysis of transit system components as well as detailed procedures to mitigate these vulnerabilities. A sample procedure to assess risk and vulnerability is outlined and contains many of the typical system components of a transit agency. A listing of procedures for mitigating risks is described as well.
RESPONSE

The overall characteristics and important considerations for responding to an incident are discussed including the transit provider’s role as a first responder. A detailed outline of the range of tasks likely to be encountered as well as key objectives for incident response (general as well as transit specific) is described as well.

Understanding the roles of other responders such is emphasized and a listing of FEMA activities is included.

Some tools for responding to an incident such as the Incident Action Plan (IAP) and the Incident Command System (ICS) is outlined and ways to adapt this system discussed. Other management tools include the incident command post and the emergency operations center are discussed as well.

RECOVERY

The blending of recovery with the ending response phase is emphasized. An overview of important aspects of recovery from an incident including service restoration (obtaining replacement parts etc.) and follow-up concerns (ongoing investigations) is discussed.
FTA PUBLIC TRANSPORTATION SYSTEM SECURITY AND EMERGENCY PREPAREDNESS PLANNING GUIDE

The FTA’s “Public Transportation System Security and Emergency Preparedness Planning Guide” states that it:

“…is based on research to identify practical steps that systems can take to be better prepared for all emergencies. These recommendations support the industry’s commitment to prevent those events that can be prevented and to minimize the impact of those that cannot.”

The guide discusses key activities that transportation organizations should perform to enhance prevention and to improve response. It also discusses the challenges of security and preparedness in the public transportation industry. The guide discusses the development of a Security and Emergency Preparedness Program (SEPP), providing guidance on how transportation systems can develop internal security, incident management systems, and external plans for coordinating with local law enforcement, other local responders, local planning agencies, and state or federal agencies. It offers an assessment by which transportation organizations can evaluate their level of preparedness and describes a methodology that can be used to conduct a threat and vulnerability assessment. It also provides sample procedures and recommendations for managing threats and highlights existing public transportation training and supervisory programs. Finally, the guide explains available design strategies and technologies to support improved public transportation security and to enhance both normal and emergency operations.

Included as appendices are an FBI vulnerability self-assessment, security contacts for the top 35 transportation systems, a detailed capabilities assessment worksheet, and sample language to assist in the preparation of a Memorandum of Understanding (MOU) between agencies.
FTA TRANSIT SECURITY PROCEDURES GUIDE

The Guide includes information on how to apply the systems approach to transit security planning and implementation; proactive materials on the prevention of security incidents; procedures for immediate and follow-up response to security incidents; and specific evaluation of a variety of special security problems including crimes against passengers, crimes against the transit system, crimes against the public (hostage, hijacking, bomb threats), and general security issues. The evaluations include information on the most important attributes of each security problem: severity, frequency, type, areas of affect, when, locations, contributing factors, solution areas, solutions/approaches, personnel cost, facility/equipment cost effectiveness and application.

The Guide is a compilation of materials for planning and improving transit security. The formation could be used by transit system planners, security personnel and managers in developing plans, procedures and capital programs. Overall, the Guide focuses on how transit agencies can prevent (mitigate) vulnerabilities and plan for incidents. Section One of the guide addresses Security Issues and Incidents: Preventing Security Incidents and Security Issues. Section Two of the guide address Security Problems: General Security Issues, Crimes Against Passengers, Crimes Against the Transit System, and Crimes Against the Public: Critical Incidents/Acts of Terrorism.

Overall, the guide address more of the criminal or mischief activities (i.e. theft, assault, vandalism, fare evasion) as opposed to terrorist activities. The document was prepared in 1993 and reprinted in October 2001. However, the reprint did not include an update based upon today's environment. The guide mentions Hostages/Hijacking/Bomb Threats but the analysis is based upon pre-9/11 assumptions.

Coordination with other agencies is discussed in a section titled “Coordination with Local Police Departments” and covers basic issues such as sharing information, setting up communications, etc. It does not discuss coordination with other transit agencies.
GUIDE TO CONDUCTING CRITICAL ASSET PROTECTION SELF-ASSESSMENTS (OHIO DOT)

This Guide was prepared to provide transit managers, operations and maintenance personnel, as well as transit police and security managers, with a set of tools to plan and conduct security assessments to address heightened threat levels. The assessments are designed to promote proactive measures:

1. To determine the agency’s level of security and emergency preparedness
2. To identify counter-measures that can be implemented to improve security performance and emergency response capabilities
3. To emphasize a management approach to security that promotes consistency, assures thoroughness, and enhances the integrity of the transit operation.

- **Planning**—The Guide indicates that it is important to coordinate with law enforcement agencies and formulate MOUs with other agencies, but it lacks a clear plan as how to coordinate with other agencies.

- **Response**—The Guide is very detailed in regards to the response activity for itself as a transit authority. For intra-agency, it only mentions that it is important to participate in preparedness training programs sponsored by FEMA, FBI and DOD.


The following figure indicates the processes involved for the mitigation action:
Overall, the Ohio DOT Guide to Conduction Critical Asset Protection Self-Assessments goes into great detail for asset identification and vulnerabilities. It also covers hardening of critical assets, what it lacks are clear procedures for intra-agency involvement and recovery.
INTEGRATED TRANSPORTATION ANALYSIS: FRAMEWORK FOR RESPONSE TO NATURAL DISASTERS & MALEVOLENT ATTACKS

This document describes the Integrated Transportation Analysis (ITA) and its purpose as a tool to predict, prevent, and mitigate impacts to a transportation network due to natural and manmade disasters. It describes the use of scenarios involving injury or damage to people, vehicles, infrastructure, and the environment. As described, the goal of ITA is to integrate law enforcement, first responders, and transportation officials at the state and local levels and provide knowledge about potential threats, both natural and manmade.

The paper provides detailed assessments of the ITA capabilities in the following areas:

- Use five framework elements – user, vehicle, infrastructure, social system, and environment
- Incident knowledge management – management of information prior to, during, and after an incident
- Vulnerability assessment and pre-incident alert
- Use of the Homeland Security Advisory System
- Information sources
- ITA Development

The paper indicates that ITA is still under development. The authors discuss the importance of establishing partnerships between state and federal agencies, national laboratories, and the private sector to finalize software development in preparation for fielding.

- **Planning**—The paper discusses how ITA is useful in preparing and predicting a potential event through the use of scenarios programmed in the software that allow planners and responders to predict potential targets and outcomes of attacks. There are no specific questions or recommendations pertaining to planning outlined in the review.

- **Response**—This document describes how ITA provides detailed analysis and recommendations for coordinated responses with inter-agency and multi-jurisdictional regions participating. The paper does not go into specifics of how the software triggers a response or what typical responses would go with certain scenarios.

- **Recovery**—The review indicates that ITA can assist response teams after an incident occurs through facilitating information exchange between agencies.

- **Mitigation**—The review describes how ITA can reassess and investigate previous incidents to provide lessons learned for use in future attacks or disasters.
MAKING THE NATION SAFER: THE ROLE OF SCIENCE AND TECHNOLOGY IN COUNTERING TERRORISM

The efficient functioning of various systems reflects achievement during the last century, however interconnectedness within and across systems also means infrastructure is vulnerable to local disruptions, possibly leading to widespread failures. The purpose of this document is to describe methods in which science and engineering can contribute to making the nation safer against the threat of catastrophic terrorism.

The document provides information and recommendations for detection, reducing vulnerability, responding to, and potential further research for each threat:

- Nuclear and Radiological Threats
- Human and Agricultural Health Systems
- Toxic Chemicals and Explosive Materials
- Information Technology
- Energy Systems

In terms of transportation the document describes characteristics of transportation systems, security systems that take these characteristics into account, and research required. A layered security systems approach is recommended, allowing security to be integrated with transportation operations. Research needs, deterrence, prevention, monitoring and mitigation, and response and recovery are discussed briefly.

Cities and Fixed Infrastructure are covered in chapter eight. Elements of city infrastructure is described including emergency management and emergency operations centers, water supply, electrical supply, information technology and communications, transportation, etc… Intra and Intergovernmental Operations are discussed related to first responders and communications needs.

The document continues with recommendations for coordination of departments and agencies to develop a framework for systems approach to counterterrorism. Coordination includes developing threat profiles of critical U.S. infrastructure, data needs, system dynamic models, and risk modeling.

Concluding the report is a section that discusses equipping the Federal Government to Counter Terrorism. This includes coordination issues, strengthening the federal governments ability to determine how science and technology can be used to counter terrorism. Finally discussed is the role of the Department of Homeland Security, and its relation to OMB and the Office of Science and Technology Policy (OSTP).
NATIONAL INFRASTRUCTURE SIMULATION AND ANALYSIS CENTER
(SANDIA NATIONAL LAB)

The NISAC is posturing itself as an organization capable to provide applicability to the Department of Homeland Defense (DHS) and national level issues using advanced computer modeling, simulation and analysis techniques. The NISAC has identified 6 self-imposed goals to provide this applicability:

NISAC Modeling, Simulation, and Analysis Goals:

1. Integrate modeling, simulation, and analysis into national infrastructure and asset planning and decision support activities.
2. Develop economic models of near- and long-term effects of terrorist attacks.
3. Develop critical node/chokepoint and interdependency analysis capabilities.
4. Model interdependencies among sectors with respect to conflicts between sector alert and warning procedures and actions.
5. Conduct integrated risk modeling of cyber and physical threats, vulnerabilities, and consequences.
6. Develop models to improve information integration.

NISAC has developed five models/simulation tools to accomplish this:

- InSIST—Indications & Warnings System and Information Sharing Tool
- DIISA—Dynamic Infrastructure Interdependencies Simulation and Analysis
- N-ABLE—NISAC Agent-Based Laboratory for Economics
- IESS—Interdependent Energy Infrastructure Simulation System
- Urban Infrastructure Suite

NISAC models/simulation tools coverage of Critical infrastructure:

- Energy—InSIST, DIISA, N-ABLE, IESS
- Info/Telecomm—InSIST, DIISA, N-ABLE, IESS, Urban Infra Suite
- Agriculture—DIISA
- Food—No current coverage
- Water—DIISA
- Public Health—Urban Infrastructure Suite
- Emergency Services—DIISA
- Government—N-ABLE
- Defense Ind Base—No current coverage
- Transportation—nSIST, DIISA, N-ABLE, Urban Infrastructure Suite
- Banking and Finance—DIISA, N-ABLE
- Chemical Industry—No current coverage
- Postal/Shipping—DIISA, N-ABLE

The NISAC tool set is a great method that could allow WMATA to develop critical node/chokepoint and interdependency analysis (NISAC Goal #3) of its system; look at modal interdependencies among sectors with respect to conflicts between sector alert warning procedures and actions (NISAC Goal #4); and provide a mechanism to conduct integrated risk modeling of cyber and physical threats, vulnerabilities, and consequences of terrorist attacks or natural disasters (NISAC Goal #5).
NAVY MODEL: INFRASTRUCTURE INDEPENDENCE & INORGANIC INFRASTRUCTURE SELF-ASSESSMENT

The Navy model is a tool intended to facilitate a self-assessment of the vulnerability of an agency/entity (such as a military base) resulting from a dependency on infrastructure external (termed Non-organic) to its operations.

About a fourth of the assessment questions are aimed at simply inventorying infrastructures with the ultimate goal of mitigating any vulnerability.

A similar number of questions are aimed at the planning arena of emergency response and largely address the inclusion of the loss of various infrastructures in planning exercises and inter-agency agreements related to restoration of service as well a very few questions aimed at the hardening of resources.

The greater number of questions is directed at mitigating infrastructure loss/damage through the provision of alternatives and the remediation of failed services.

The tool does not address the response aspects of emergency preparedness.

The other aspect of the model, the Non-organic assessment outlines basic procedures for physically identifying critical (physical) infrastructure points in the field with suggestions for mitigating these critical locations through increased security and consultation/agreements with service providers.

Overall, the navy model tool addresses regional aspects of infrastructure in that it considers various types of services. However, the interdependent nature of these is not considered in the assessment. In addition the tool largely does not address the organizational, inter-jurisdictional aspects of emergency response, a key part of emergency preparedness for the Metro region.

The model appears particularly well suited for assessing the vulnerabilities of telecommunications and electric power, where the question sets are more comprehensive than that for transportation infrastructure.

The question set relating to logistics services appears useful as well, as it addresses the consideration of the continuation and mitigation of aspects of services not covered in the “hard” infrastructure aspects.

INFRASTRUCTURE

By means of a set of questions, the procedure addresses aspects of various infrastructures including electric power, telecommunications, natural gas, transportation, water, and logistics support. A brief look at the scope of questions regarding the various infrastructure’s related to the Metro (electric power, telecommunications, transportation, and logistics support) follow.
ELECTRIC POWER

The range of questions provides a comprehensive look at the nature of dependence on electrical power (an essential component of the metro operations) and measures to mitigate and recover form its loss.

A few questions are aimed at assessing the physical nature of the connection (single or dual connection) and the identification of the electric service provider installations that are critical to facility operations.

Various questions address planning for the loss of service such as the inclusion of power loss (as well as the service provider) in emergency response planning and inter-agency priority requirements/agreements with the provider for power restoration.

The bulk of the remaining question address recovery from service loss through strategies to reconstitute and continue operations (such as formal agreements for the provision of spare parts in emergency situations) and the provision of alternatives to mitigate power failure (such as the availability of emergency backup power).

TELECOMMUNICATIONS

The nature and scope of the questions are nearly identical to those for electric power infrastructure and consider aspects of both conventional and wireless communications.

A few questions are aimed at assessing the physical nature of the connections (single pathway or switch) and the location(s) of critical components.

A number of questions address planning for the loss of service either directly or through the loss of power, the inclusion of the service provider in emergency response planning and inter-agency priority requirements/agreements with the provider for service restoration.

The greater part of the questions consider the mitigation of service losses through the availability of alternative communication networks/arrangements (such as Telecommunications Service Priority (TSP) -developed to ensure priority treatment for the Nation's most important telecommunications services- the Government Emergency Telecommunications (GETS), the Defense Switched Network (DSN), and other priority communication networks such as NIPRNET, SIPRNET and JWICS) that may be available only for defense related entities and not applicable at all to the Metro region.

TRANSPORTATION

The questionnaire addresses various modes of transportation including rail, air, ports, and highways.

About half of the questions (21) are aimed at simply inventorying (external) infrastructures with the ultimate goal of identifying and mitigating their vulnerabilities.

The remaining questions are aimed at mitigating the loss of infrastructure through the consideration/development of alternatives.
The non-organic model outlines procedures for identifying critical (considering only highway) structures such as bridges and tunnels and mitigation measures such as seeking out increased surveillance of (critical) structures by itself or through other agencies (inter-agency agreements).

LOGISTICS SUPPORT

The questions here consider the impact on operations related to the availability of various vendors during emergency situations such as medical supplies and treatment (vendors for spare parts etc?), the availability and use of alternate vendors, as well as priority requirements and the consideration/development of alternatives for service provision.

A number of questions are directed to the identification of providers, the nature of the agreements (i.e. sole-source) and the priority requirements for service provision.

Other questions consider planning for the loss of logistic services and inter-agency agreements for service provision.

Another group of questions involve the recovery and mitigation of service loss thru the consideration/development of alternative providers.
PROTECTING OUR TRANSPORTATION SYSTEMS: AN INFORMATION SECURITY AWARENESS OVERVIEW

Surface transportation systems increasingly rely on a growing number of sensing, computing, and communications capabilities -- collectively known as information technologies. The application of these technologies to our transportation infrastructure has been termed Intelligent Transportation Systems (ITS). Over the past several years, ITS have clearly demonstrated their ability to improve the efficiency of moving goods and people, improve the safety of our transportation system, and provide the public with information on alternative modes of travel.

Because the application of these information technologies has proven to be cost-effective, they are increasingly deployed by state and local governments. Unfortunately, the threats (i.e., events that can harm the system) and vulnerabilities (i.e., weaknesses in system implementation) affecting these technologies are developing almost as rapidly as the technologies themselves, thus the need for information security.

The report first provides a number of reasons why a transportation agency should be concerned with information security. The report identifies six categories of those who should be concerned: Owners, Developers, Managers, Operators, Users, The Public.

Next, the report presents hypothetical, yet realistic, events that illustrate the potential impacts to various ITS services that result from inadequately secured information technology system. Salient examples to public transportation include Travel and Transportation Management, Travel Demand Management, Public Transportation Operations, Electronic Payment, Emergency Management and Advanced Vehicle Control and Safety Systems.

After presenting hypothetical events, the report document what can be done about these vulnerabilities. These security services are divided into two categories. First, the Technical Security Services includes items such as Confidentiality, Authentication, Data Integrity, Non-repudiation, Access control, Accountability and Availability. Second, the Non-technical Security Service includes items such as Administrative Security, Personnel Security and Physical Security.

Finally, the paper combines these security services into an overall Information Security Program. Topics covered include:

- Strategic Security Planning
- Security Policy Analysis and Definitions
- Secure Solutions Integration
- Security Awareness, Education & Training
- Security Management
- Security Assessment an Testing
In general, this report focuses on the security and vulnerabilities of information, data and the components associated with it. It is not specific to one mode of transportation or agency size. It provides more high-level discussion points rather than a detailed security or vulnerability assessment. It mentions the inclusion of inter-jurisdictional planning and coordination but only at a fairly high level. Overall, this tool provides a necessary mechanism to begin the discussion of securing ITS information technology. However, it does not provide the necessary specifics to conduct an overall vulnerability assessment or begin to address inter-agency or inter-jurisdictional issues.
PROTECTING SURFACE TRANSPORTATION SYSTEMS AND PATRONS FROM TERRORIST ACTIVITIES AND SERIOUS CRIMES

The objective of the project is the creation of a best practices textbook describing the most effective security measures and response procedures. In order to execute this task, four case studies namely the Paris Subway System (St. Michel), Amtrak (Sunset Limited), The New York Transit Authority (Contingency Planning for Emergency Response), The Metropolitan Atlanta Rapid Transit Authority, (Olympic Games 1996) explored. Each case study examines three issues i) policies and practices in effect prior to the incident (pre-incident preparedness), ii) the response to the event or heightened threat environment and iii) the recovery efforts.

A format to facilitate comparisons comprise - a description of the transportation system itself, all aspects of existing security such as threat assessment security organization, personnel, procedures and training, environmental design, security technology, emergency communications and the role of the public, crisis management planning, liaison with other authorities and the immediate response to attacks or threats including additional security, emergency response, restoration of services, lessons learned and problems identified.

- **Security Technology**—The case studies and surveys indicate that all of the larger operating entities examined have dedicated security forces departments. Conduct visible patrols as well as undercover surveillance. In addition, the systems make use of communication devices such as radios, centralized electronic control centers, CCTV, as effective deterrent measures. Moreover, intrusion sensors and alarms monitored by control centers, use of technology to provide accurate location of all trains and buses and security personnel are in place.

- **Advance Planning**—The case studies show that advance planning is essential to ensure a coordinated and effective response to a threat or attack. Frequent joint exercises involving all concerned agencies identify potential problems in advance and ensure readiness.

- **Environmental Design**—The case studies identify a number of examples of environmental design to facilitate surveillance, increase physical security, eliminate potential hiding places, and reduce sources of fragmentation, combustible material and materials that produce toxic fumes.

- **Communications**—The case studies indicate that all the agencies under review have multi-mode communications systems to ensure communications during routine operations and crisis situations. These systems include multiple radio networks, cellular, landlines and public address systems.

- **Training**—All of the operating entities reviewed in the case studies placed great emphasis on training. This includes training of personnel, regular drills, tabletop exercises, no-notice response and full-scale simulations.

- **Public Involvement**—The transportation systems examined have decided to make public part of their overall security effort by posting signs and broadcasting warnings that urge patrons not to leave their luggage or parcels unattended and to immediately notify the authorities of unattended or suspicious parcels.
- **Augmented Security**—In order to augment security following a terrorist attack or in times of heightened threat, systems under review increase the visible presence of security personnel, drawn from different agencies at the both the local and national level.

One of the biggest issues for any transit agency in developing and implementing an effective “crisis management” program whether it is aimed at criminal activity or natural disasters is coordination with other agencies and organizations that are expected to be part of response scenario. Depending on the magnitude of the problem, these may include: - Local law enforcement, Fire Departments, Ambulance and Emergency Medical Teams and related health services, Local Government Emergency Management Office, Red Cross, Crisis Counselors, State Emergency Management Office, DOT, Public Safety, National Guard, FBI and FEMA.
PUBLIC TRANSPORTATION SYSTEM SECURITY AND EMERGENCY PREPAREDNESS PLANNING GUIDE: ANALYSIS OF CRITICAL RAIL AND BUS ASSETS (TCRP PROJECT J-10A)

To supplement information provided in the Public Transportation System Security & Emergency Preparedness Planning Guide, TCRP Project J-10A(1), McCormick, Taylor & Associates have compiled a CD-ROM contains over 200 documents, most of which have been published since September 11, 2001, by Federal and state transportation, law enforcement, emergency management, and military agencies. These documents explain the roles and responsibilities of the 47 Federal agencies involved in homeland security, and provide useful technical assistance on a range of security and emergency management subjects. Sample procedures and model plans are included in on the CD.

Another tool that may prove very useful is the Analysis of Criticality Checklist. Individual checklists are provided for both rail and bus transit assets. The checklist provides the ability to determine the level of impact that various elements of the transit network (e.g., transit station or multi-modal transfer point) would have on both passengers and the transit systems in the event of loss of service. The scale used for this analysis is high, medium, or low. Categories of rail systems that are analyzed with this tool include:

- Station;
- Transit center;
- Multi-use/inter-modal connection;
- Vehicles (rail cars and support equipment);
- Track/track structure;
- Signals, switches and inter-lockings;
- Communications-based train control or protection systems;
- Grade crossings and automated warning devices;
- Electrification systems;
- Parking lots;
- Operations control center;
- Revenue collection facilities;
- Train storage yards;
- Service and inspection facilities;
- Heavy maintenance facilities;
- Wayside support and maintenance facilities;
- Ancillary Facilities;
- Administrative facilities;
- Employee parking lots; and
- Transit police facilities and communications systems.
Categories of bus system that are analyzed with this tool include:

- Terminal/station
- Transit center
- Multi-use/inter-modal center
- Bus stops and shelters
- Vehicles
- Roadways
- HOV and dedicated bus lanes
- ITS and supporting equipment
- Parking lots
- Bus garages and storage facilities
- Heavy repair facilities
- Service and inspection facilities
- Inventory and storage facilities
- Alternative fuel facilities
- Operations control center
- Communication systems
- Revenue collection facilities
- Administrative facilities
- Employee parking lots
- Transit police facilities
PUBLIC TRANSPORTATION SYSTEM SECURITY AND EMERGENCY PREPAREDNESS PLANNING GUIDE: BASELINE SECURITY CHECKLIST (TCRP PROJECT J-10A)

To supplement information provided in the Public Transportation System Security & Emergency Preparedness Planning Guide, TCRP Project J-10A(1), McCormick, Taylor & Associates have compiled a CD-ROM contains over 200 documents, most of which have been published since September 11, 2001, by Federal and state transportation, law enforcement, emergency management, and military agencies. These documents explain the roles and responsibilities of the 47 Federal agencies involved in homeland security, and provide useful technical assistance on a range of security and emergency management subjects. Sample procedures and model plans are included in on the CD.

Among the tools provided on the CD that might prove most useful in conducting vulnerability self-assessments is a Baseline Security Checklist. This tool is generic and would need to be tailored by WMATA to meet its unique and individual needs. The primary objective of the Baseline Security Checklist is to help each system identify its current baseline regarding security and emergency preparedness activities. In addition, a Detailed Worksheet provides additional information to help transportation personnel determine the applicability of a particular Checklist Item to their operation. The Baseline Security Checklist provides a series of “yes or no” questions in the following categories:

- Security awareness and threat management;
- Security and preparedness planning;
- Security and preparedness management;
- Threat and vulnerability assessment;
- Physical security; and;
- Emergency response capabilities.
A STATE DOT GUIDE TO HIGHWAY VULNERABILITY

This guide provides a starting point to help state DOTs identify and mitigate the vulnerability of and consequences to highway transportation assets from terrorist threats. It proposes a methodology for State DOTs to assess vulnerability of physical assets, develop countermeasures to deter, detect, and delay consequences of terrorist’s threat, estimate capital and operating costs of countermeasures, improve security ops planning for protection against future acts of terrorism. It identified six steps to an overall vulnerability assessment:

1. Identify critical assets
2. Assess vulnerabilities
3. Assess consequences
4. Identify countermeasures
5. Estimate countermeasures costs
6. Review operational security planning

However, the vulnerability assessment process only addresses planning methodology, and does not discuss response, recovery, or mitigation. Below is a detailed summary of its planning approach:

- **Planning**—The critical asset identification and protection assessment tool provides a single agency with the methodology to enhance security and protect infrastructures deemed critical by personnel. The process does not address interagency agreements. While focused on a single agency requirements the methodology proposed does briefly consider interagency agreements, however only notes the need to clarify roles and responsibilities. There exists potential to address multi-agency facilities through inclusion of various stakeholders during asset identification decision making. A security operational plan is developed based on the U.S. Army Physical Security Field Manual. The Operational Plan addresses infrastructure access restrictions, countermeasures, and gives brief discussion of contingency planning.

- **Resources**—Again based on single agency needs, potential countermeasures are defined by the Army Field Manual 3-19.30—Physical Security. Three functions of countermeasures are proposed: (1) Deterrence; (2) Detection; (3) Defense. These functions are applied to potential countermeasures based on the perceived need level. Countermeasures tend to address processes, such as increased inspection; surveillance, access restrictions, training, and security systems such as motion sensors.
Appendix B: Assessment Criteria

PLANNING AND PREVENTION

Agency/Organizational

1. Intra-agency plans/agreements activities?
2. Inter-agency planning activities?
3. Inter-jurisdictional planning activities?
4. Inter-modal planning activities?
5. Table-top or scenario exercises?
6. Field Training?

Resources

7. Resource sharing?
8. Resource allocation?
9. Equipment inventories?
10. Hardening of resources?
11. Does the tool address the issue of Resource Needs Analysis?
12. Equipment?
13. Communications?
14. Staff?

RESPONSE

Agency/Organizational

15. Does the assessment tool address the analysis of multi-agency operations, and or transportation operations?
16. Fire
17. Police
18. Emergency Medical Services
19. Other transit property
20. Other transportation agency
21. Federal law enforcement/investigative organizations
22. Does the assessment tool consider command structures?
Resources

23. Does the assessment tool consider a range of natural and/or man-made disasters (intentional, non-intentional).
24. Does the assessment tool address inter-jurisdictional and/or inter-disciplinary use of resources?
25. Equipment?
26. Communications?
27. Staff?

RECOVERY

Agency/Organizational

28. Does the assessment tool address working relationships with multiple agencies?

Resources

29. Does the assessment tool address reconstitution of services.
30. Does the assessment tool address strategies for continuation of services/operations?

MITIGATION

Agency/Organizational

31. Does the assessment tool address ongoing working relationships with multiple agencies?

Resources

32. Does the assessment tool address remediation of failed services?
33. Does the assessment tool address replacement of failed services?
34. Does the assessment tool address the identification of infrastructure vulnerabilities?
35. Does the assessment tool address measures for hardening infrastructure?
36. Does the assessment tool address alternatives for loss of infrastructure or services?
Appendix C: Hybrid Self-Assessment Tool