Government Mission Survivability and Continuity

Recommendations from Balanced Survivability Assessments

Gregory Gilbert CBCP
Emergency Operations and Continuity Specialist
Contractor Support for Defense Threat Reduction Agency (DTRA)

DTRA Mission

“The mission of the DTRA is to safeguard the United States and its Allies from weapons of mass destruction by providing capabilities to reduce, eliminate, and counter the threat and mitigate its effect.”

Reference: DTRA Charter
DoDD 5105.62, 28 November 2005

Balanced Survivability Assessments

- Integrated, multidisciplinary, mission-survivability assessments to identify vulnerabilities of critical national/theater mission systems and recommend mitigations
  - Focus is on understanding entire system (details to architecture)
  - Focus is on mission survivability with an emphasis on identifying single point vulnerabilities (SPVs)
  - Performance (not compliance) based assessments
  - Considers entire threat and hazard spectrum
  - Team is matched to site needs
  - 2–3 weeks onsite plus post-site analyses
  - Products: out-briefing and report identifying vulnerabilities, impacts, and recommended mitigations
  - Frequently leveraged to support CIP programs
  - Customer controls product distribution

Risk Management Process

<table>
<thead>
<tr>
<th>Threat/Hazard Assessments</th>
<th>+</th>
<th>Vulnerability Assessments</th>
<th>+</th>
<th>Criticality Assessments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local/Unit</td>
<td></td>
<td>State</td>
<td></td>
<td>Federal</td>
</tr>
<tr>
<td>AT/FP</td>
<td></td>
<td>BSA</td>
<td></td>
<td>CI Staff</td>
</tr>
<tr>
<td>Red Team</td>
<td></td>
<td>Local VA</td>
<td></td>
<td>DIA/CIA</td>
</tr>
<tr>
<td>Etc.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Risk Assessments

Commander / Asset Owner

Commander
Mission Essential Functions and Tasks (MEFs/METs)
Single Point Vulnerability

SPV

Equipment, processes, procedures, infrastructures, and/or key positions that, if destroyed or denied, would result in the loss or severe degradation of mission.

System Survivability Assessment

HAZARDS & INCIDENTS

- ACCIDENTS
  - Fire
  - Hazmat Release
  - Natural Disasters
  - Earthquake

- Equipment Failures
- Disruptive Actions
- Chemical Weapons
- Hostile Attacks
- Cyber-attack

SYSTEM ASPECTS

- Cyber Security
- Mission Systems
- Physical Security
- Utilities/Endurance
- Telecommunications
- Structural Protection
- Emergency Response
- Continuity of Operations
- Information Operations
- Operational Security
- WMD Protection
- Fire Prevention

OUTPUT

- Integrated, multidisciplinary, mission-survivability assessments
- Focus on vulnerabilities with emphasis on SPVs

Outbriefing
- Report
- Continuing Assistance
- Lessons Learned

Types of Systems and Facilities Assessed

- Command & control architectures and sites
- Operations centers
- Information technology architectures and sites
- Telecommunications architectures and sites
- Intelligence collection and fusion centers
- Missile defense sites
- Deployment sites
- Depots and weapons storage sites
- Logistics operations centers
- Airfields
- Naval Bases
- Strategic ports
- DoD manufacturing sites
- Medical research facilities
- Stockpile sites
- Navigation, positioning, and timing sites
- Dams

BSA Impact

Example projects where BSA results provided compelling justification for survivability improvements

<table>
<thead>
<tr>
<th>Funds</th>
<th>Customer</th>
<th>Project</th>
</tr>
</thead>
<tbody>
<tr>
<td>155.0</td>
<td>Service Communications Facility</td>
<td>New building and equipment</td>
</tr>
<tr>
<td>49.0</td>
<td>Service Communications Facility</td>
<td>Communication and building upgrades</td>
</tr>
<tr>
<td>127.9</td>
<td>Headquarters Complex</td>
<td>IT &amp; Infrastructure upgrades</td>
</tr>
<tr>
<td>108.6</td>
<td>Global Communications Facility</td>
<td>Facility and network upgrades</td>
</tr>
<tr>
<td>156.0</td>
<td>CDFP Site</td>
<td>Completed, ongoing, planned upgrades</td>
</tr>
<tr>
<td>8.4</td>
<td>Research &amp; Development Facility</td>
<td>Information operations upgrades</td>
</tr>
<tr>
<td>27.5</td>
<td>Headquarters Complex</td>
<td>Infrastructure upgrades</td>
</tr>
<tr>
<td>14.0</td>
<td>Headquarters Complex</td>
<td>Facility and infrastructure upgrades</td>
</tr>
<tr>
<td>10.1</td>
<td>Satellite Ground Station</td>
<td>Facility and infrastructure upgrades</td>
</tr>
<tr>
<td>1.4</td>
<td>Weapons Storage Facility</td>
<td>Site, building and access upgrades</td>
</tr>
</tbody>
</table>
Major BSA Recommendations

• Include mission survivability/resiliency in facility design
• Monitor and Limit open-source and Internet information
• Establish counter-surveillance programs and awareness
• Understand threats/hazards, their probabilities, and impacts
• Avoid predictable security routines; ensure randomness in procedures/operations
• Ensure standoff/construction provides survivable blast protection
• Ensure information networks are protected from insider and external threats
• Ensure communications, information, and utility systems are redundant and diverse
• Ensure fire and hazard protection is consistent with mission criticality
• Ensure lighting protection and grounding systems are effective and maintained
• Ensure mail and parcel handling prevents the introduction and spread of contaminants
• Implement and exercise emergency action and COOP plans

Critical assets need to be protected commensurate with their value to the Nation

Sharing BSA Experience

• Objective is to ensure that information on critical vulnerabilities and best practices for mission survivability reaches decision makers
• BSA results are transferred to the DoD (and Agency) communities in many ways
  • Out-briefs and reports
  • Lessons learned and trends products
  • "Designing for Mission Survivability" guidelines (~44 copies distributed to customers since August 2010)
  • Special reports and "roll-up" briefings to DoD leadership
  • Design reviews (COCOMs, Agencies, etc.)
  • Support to customers using databases to track vulnerabilities
  • Participation in working groups
  • Policy document reviews

BSA Information Operations Assessment Tool

• Customer discretionary and tailored assessment of customer defined networks
  • Precisely identifies IO/IA vulnerabilities w/o impacting operations
  • Provides in-depth understanding of networks and IT systems security
  • No penetration testing while connected
• Tools include:
  • Methodology based on NSA, DoD, NIST, BSA and commercial best practices
  • NSA developed Blue Team vulnerability tool suite
  • Commercial and open-source modeling and vulnerability scanning tools
  • BSA IA toolkit process
    • Detailed pre-coordination – formal agreement Letter/scoping worksheet
    • Scan at "non-peak" times with strict schedule control
    • End-to-end data protection
    • Encrypted external drives/volumes, secure GFE laptops, and DTRA air-gapped SCI LAN
  • Critical findings immediately reported to customer while on-site
  • Accomplishments – identified potential malware, unauthorized and non-secure network activities, and vulnerable configurations; 4 years with no adverse impacts/outages

BSA Trends Analysis

• Compile, statistically analyze, and report long-term survivability trends in:
  • Physical security, surveillance, structural protection, WMD/Hazmat, electromagnetics, utilities, telecommunications, information systems, emergency operations, COOP, and architecture resiliency
  • Aspects with highest historical ratings
    • Utilities endurance and capacity
    • Architecture resiliency
    • Structural blast resistance
    • Utilities redundancy and diversity
  • Aspects with lowest historical ratings
    • Open source information
    • Lightning protection
    • External signatures/vulnerabilities
    • WMD detection, identification, warning
    • External electromagnetic protection
    • Information systems and data
## Recommendations by Assessment Area

- Threats and Hazards
- Surveillance
- Physical Security
- Emergency Operations
- Fire Protection
- Structural Response
- Telecommunications
- Information Operations
- Utilities
- WMD/Hazmat
- Electromagnetic Protection
- Defense Industrial Base
- Mission Restoral
- Population Protection

## Threats and Hazards

- Consolidate threats and hazards analysis; ensure it drives risk management
- Managers and security personnel should understand threats/hazards, their probabilities, and impacts; stay current
- Avoid "rationalizing away" threat/hazard risk
- Avoid predictable security routines; ensure randomness in procedures/operations
- Monitor infrastructure hazards and cyber threats
- Avoid an “all threats/hazards” mentality that overlooks risks
- Accidents, electromechanical failures, and human errors are the most likely incidents; include them
- Ensure contract and business disruptions risks are considered

## Surveillance

- Monitor, control, and mitigate infrastructure and operational information available on the Internet
  - Imagery, organization websites, organization publications, acquisition documents, budget and program documents, resumes... on .mil, .com, .org, .net, .gov
- Establish OPSEC inside and outside the perimeter
  - Implement and enforce rules to establish an OPSEC culture
- Control and maintain outer perimeter and facility physical access
- Ensure communications lines cannot be easily identified
- Implement surveillance detection programs
  - Monitor external activities
  - Promote a culture of awareness and reporting

## Physical Security

- Ensure defense is layered and integrated to detect, assess, delay, deny, and respond
- Ensure physical and electronic security systems are properly installed, integrated, utilized and provide adequate coverage
- Implement an immediate visual assessment capability
- Implement internal circulation controls that account for insider threats and do not over-rely on employee “trust”
- Ensure external lighting coverage is effective
- Control personnel and vehicle circulation in/around critical areas/resources
- Ensure personnel managing electronic access control systems are properly vetted/cleared
Physical Security

- Protect security control centers; ensure alternates are adequate
- Prevent unauthorized vehicle and pedestrian access to installation and compound perimeters
  - Install and use active vehicle barriers, ensure they can be activated quickly enough to prevent access
  - Install effective passive vehicle barriers
  - Physically and electronically verify Id cards
- Implement effective vehicle vetting and inspections
  - Do not grant commercial vehicle access using a printed bill of lading or similar document
  - Verify deliveries
  - Implement explosives detection capabilities

Emergency Operations

- Develop and implement effective emergency plans
  - Address likely threats/hazards
  - Coordinate with support organizations
  - Leverage immediate response actions available to organic personnel
- Continuously monitor infrastructure hazards; ensure incident warnings/indications are properly assessed
- Train and exercise plans to ensure planning is effectively implemented
- Ensure evacuation and shelter-in-place planning is integrated and tailored to threats/hazards
- Enforce prevention and safety programs; do not allow a culture of acceptance

Fire Protection

- Ensure protective design is commensurate with criticality and integrated with operations
- Maintain detection and suppression systems and configurations
- Ensure fire detection systems provide early warning and are continuously monitored locally
- Control fire loads and ignition sources
- Ensure fire extinguisher deployment is tailored to systems and fire risks
- Implement effective immediate actions training

Structural Response

- Do not allow vehicles to park under or too close to buildings
- Avoid building designs that install glass curtain walls
  - Greater risk of injuries (~80% of casualties from flying glass)
- Ensure construction and staging area security and inspections prevent exposing critical buildings
**Structural Response**

- Ensure critical structures have sufficient stand-off from public roads and perimeter fences
- Ensure building designs identify appropriate strength and threat standoff requirements
  - Do not accept minimum criteria
- Post-construction mitigations are extremely expensive

**Telecommunications**

- Ensure communication networks are resilient and survivable:
  - Include redundant system components
  - Avoid multiple series single points of failure
  - Do not collocate redundant systems and components
  - Include physical diversity between primary and secondary circuits
  - Route cabling through physically diverse manholes and building penetrations
- Ensure site internal and external fiber diagrams are accurate, identify physical locations, and are maintained
- Hardened communications: ensure supporting systems are also hardened

**Information Operations**

- Ensure system and network components have redundancy and physical diversity
- Integrate coordinated computer network defense and incident handling response
- Ensure network security protections and monitored network security devices effectively protect systems
- Manage configuration to avoid significant end-of-life hardware and software issues in Program of Record systems and customer-controlled networks
- Production networks should not be connected to software development networks; avoid Internet connections
- Implement effective malicious insiders protection
- Implement effective IA measures on non-traditional networks
  - Utility control systems, electronic physical security systems

**Common System/Facility Themes**

- Reliability (N+1, 2N, etc.) does not equal survivability
- Does not account for threats, hazards, and accidents
- Construction, upgrade, and renovation project requirements should consider survivability, resiliency, and integrate operations

**System and Component Collocation**

- Redundancy and Diversity
  - Do not collocate redundant systems and components
  - Include physical diversity between primary and secondary circuits
  - Route cabling through physically diverse manholes and building penetrations
- Ensure site internal and external fiber diagrams are accurate, identify physical locations, and are maintained
SCADA* Systems

- Properly accredit, monitor, and manage SCADA
- Ensure configuration provides defense-in-depth
- Avoid non-secure remote dial-up access modems; manage external connectivity
- Control vendor access; ensure his laptop, software, and data are scanned
- Provide SCADA system redundancy
- Ensure SCADA does not tie into site networks
- Strictly segregate control and monitoring permissions

Utilities

- Implement redundant and diverse utility system designs
- Avoid single-threaded distribution paths between components
- Protect collocated components and single threaded paths equal to supported operations
- Protect external equipment to include transformers, switchgear, and cooling towers
- Ensure emergency generators can be manually started and aligned to loads
- Ensure utility systems have the required capacities
- Two independent water sources to cooling towers
- Protect, control, and manage SCADA systems to mitigate insider and external threats
- Ensure preventive maintenance is identified and accomplished
- Manage configurations (“as-built” drawings, technical documentation, etc.) to safely and efficiently operate/maintain systems, prevent compromising resiliency, and enhance recovery

Utilities

- Current technology permits dual-power-cord input to electronic devices; redundant and diverse power supply inputs improve survivability
- Ensure dual-power-cord electronic devices are not fed single-threaded power from the same power panel/power distribution unit

WMD

- Ensure building make-up air intakes are elevated and protected
- Implement an effective warning, identification, and assessment capability
- Install a capability to quickly shut down facility ventilation
- Ensure emergency response plans address CB/hazmat threats and hazards
- Integrate into shelter-in-place and evacuation plans
- Ensure response is linked to force protection conditions
- Identify hazards and threat vectors; plan to these
- Stock and deploy sufficient CB/hazmat protection equipment and medical supplies
Mail and Package Delivery
- Accept and process all delivery (USPS, FedEx, UPS, etc.) externally from facilities supporting operations or containing large populations; delivery facility/room design should include:
  - Negative pressure ventilation
  - Frangible exterior wall
  - Independent HVAC* system
  - Protective/decontamination equipment/supplies
  - X-ray, radiation, and explosives detection equipment
  - Procedures to safely examine or open mail
- Implement suspicious package handling procedures and training
- Install a capability to rapidly shutdown HVAC to contain releases

* HVAC = heating, ventilation, and air conditioning

Electromagnetic Protection
- Install and maintain effective facility, systems, and component grounding
  - Must address life safety and protect systems
- Install, maintain, and test effective lightning protection systems
- Assess lightning risk
- Must address life safety and protect systems
- Electromagnetic pulse - contact DTRA POC if an EMP requirement is known or perceived

Defense Industrial Base
- Avoid single-source and foreign-source suppliers
- Just-in-time delivery introduces potential risks
  - Only a few days supply of parts on hand
  - Penalties for early shipping to downstream customers
- Ensure replacing specialized manufacturing equipment have acceptable lead times
- Ensure government has insight into and monitors subcontractors

Mission Restoral
- Ensure planning addresses damage assessment procedures and is coordinated with supporting organizations
- Ensure personnel, equipment, services, software, documentation, and supplies required to restore a mission are understood and available
- Understand lead time required to obtain major items and critical supplies
- Explore alternate sources to obtain major items and critical supplies
- Maintain systems and software configuration data to avoid hampering restoral efforts
Population Protection

- Understand numbers and locations of people in buildings and movement patterns to:
  - Implement planning that avoids movement into or through threats and hazards
  - Avoids hampering response efforts
- Ensure community facilities (clubs, athletic fields, malls) are not forgotten
- Limit special-event information and distribution
- Avoid “rationalizing away” threat/hazard risk
- Avoid siting high-occupancy buildings sited near public roads and installation perimeters
- Implement and coordinate effective emergency planning and training
  - Detect, assess, warn, direct, respond, shelter, evacuate

Programming and Investing in Survivability

Government COOP Myths, Legends & Reality

Myths and Legends
- COOP is only relocation
- COOP is only IT disaster recovery
- It can’t happen here
- Asymmetric threats don’t live here
- They can pick up the load
- It is unaffordable, so we will accept the risk
- We have a disaster plan
- COOP Plan for ERG = COOP plan for entire enterprise

Reality
- COOP is a part of prevention, response, and recovery
- COOP is infrastructure, information, IT, communications, and people
- It will happen with a real probability and a real impact
- Planning for an asymmetric world is required
- They don’t know they are to pick up the load and have never exercised it
- Accepting risk will never lead to a funded requirement
- Disaster planning is about response and recovery, not continuity planning
- Missions are not things, resources are things; COOP planning manages mission risk by assuring things

Continuity of Operations

- COOP planning should:
  - Be driven by critical mission requirements (recovery time and point objectives) and risk
  - Implement what needs to be done not what can be done
  - Address likely hazards/threats and impacts; an “all threats/hazards” approach creates gaps and inefficiencies
  - Balance resiliency and leverage response; avoids inefficiencies
  - Be properly staffed, resourced, exercised and supported by leadership
  - Train COOP planners/leadership
- Inadequate business process and impact analyses will not yield effective planning
- COOP programs must be coordinated and integrated within communities
  - Dependencies and interdependencies need to be mapped
Continuity of Operations

• Organization COOP planning must be coordinated and integrated with higher level COOP and supporting organization COOP
• COOP planners need to understand Federal and Department strategies, requirements, and implementation guidance
• Backup systems should not be collocated and should be tested to ensure correct data is properly stored and accessible
• Implement effective IT disaster recovery plans and data backup procedures that are coordinated with recovery time or point objectives and devolution, transfer, relocation site selection and operations
• Ensure network failover is adequately tested; not just tested with primary system still online

Government Mission Essential Function Decomposition

MEF’s and METs are not things. Resources are things. COOP planning manages resources by assuring things.

MEF COOP requirement is driven by its critical resources’ asset with the shortest RTO
• Establish MEF continuity requirements via MET criticality; plan and allocate at the resource level to manage MEF risk

Government COOP Requirements Development

• Business process and impact analyses
  - Model enterprise structure and resources to link systems, architecture, and infrastructure to essential functions and tasks (BPA)
  - Determine resource threats/hazards and probabilities (threat/hazard analysis)
  - Determine resource impacts (vulnerability assessment)
  - Determine risk; Risk = f(threat/hazard probability & impact) (risk assessment)
  - Determine criticality measures (time, impact, etc.) that drive COOP planning requirements, mitigation alternatives, and strategies
  
  Program, products, processes, organization, and infrastructure documentation and data review
  - Map the enterprise and infrastructure
  - Develop threats and hazards data

MEF/MET interviews
• Map MEFs to METs to Resources
• Determine criticality of Resources
• Map Resources to MEFs
• Risk analysis, planning, vulnerability and impacts

Who, what, where, when, how

Points of Contact

• Mr. William Austin, Chief, BSA Branch, DSN 427-9761 or 703-767-9761, email: william.austin@dtra.mil
• Mr. Gregory Gilbert, Emergency Operations Lead, DSN 427-9719 or 703-767-9719, email: gregory.gilbert_contractor@dtra.mil