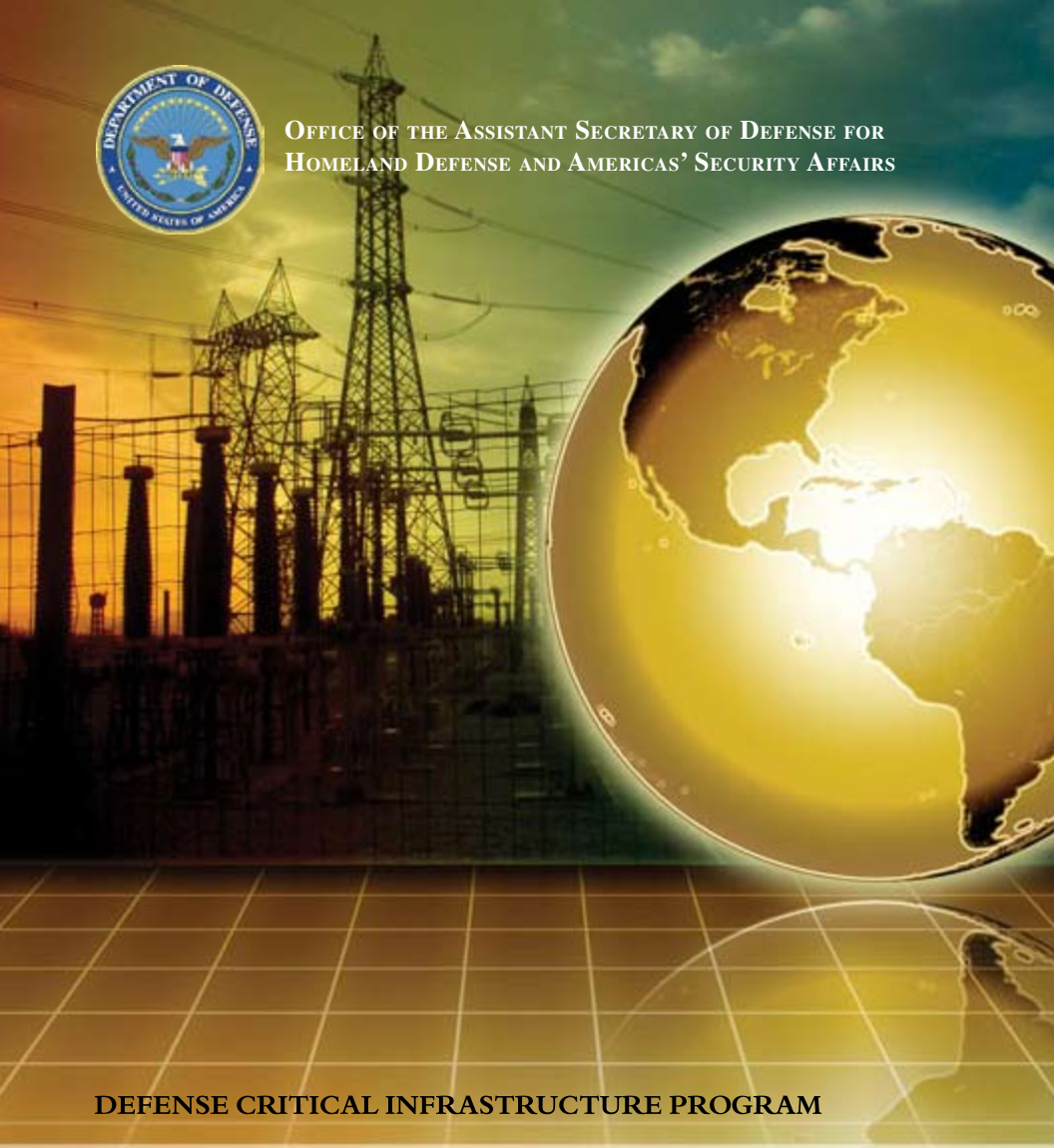


Office of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs

DEFENSE CRITICAL INFRASTRUCTURE PROGRAM

Infrastructure Resiliency Guide

Reduce Your Vulnerabilities and Make Your Infrastructure Stronger

Version 1.0 - May 2007

Reducing Risk...
Improving Resiliency

TOC Table of Contents

Preface

Events such as the terrorist attacks of 9/11 and the hurricanes of 2005 have taught us many valuable lessons concerning our reliance on infrastructure. The Department of Defense has institutionalized a process to identify our dependencies on infrastructure networks and improve their resiliency through the Defense Critical Infrastructure Program. The goal of the Defense Critical Infrastructure Program is to ensure that the Department of Defense critical assets are available when required. To implement this program, we conduct in-depth analysis and assessments of what is critical, how it is threatened, and the associated vulnerabilities.

Over the past several years, the DoD has identified common vulnerabilities to infrastructure through conducting vulnerability and risk assessments and refining the assessment process. This Infrastructure Resiliency Guide is a compilation of our findings from the assessments on vulnerabilities and corrective actions.

We hope you will use this document to review the infrastructure networks available to you and implement these corrective actions where appropriate. In doing so, we can improve the Department's overall infrastructure resiliency.

This guide will be periodically updated and distributed. We welcome your suggestions for improving the usefulness and content of the guide. Please e-mail your suggestions to rss.dcipoffice@osd.mil with the subject line of "Infrastructure Resiliency Guide."

Peter F. Verga
Acting
ASD(HD&ASA)

PURPOSE

The Defense Critical Infrastructure Protection (DCIP) Infrastructure Resiliency Guide provides information for improving the resiliency of infrastructure systems and solutions for reducing risks to infrastructure networks.

This guide is the result of numerous commercial infrastructure vulnerability assessments conducted by multiple agencies and organizations within the Department of Defense (DoD).

This document was produced in consultation with subjectmatter experts (SMEs) in the various infrastructures identified in the document and with trained vulnerability assessors to identify common weaknesses of infrastructure systems.

INPUT ACKNOWLEDGEMENTS

This document was created in coordination with inputs from:

- Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics (OUSD(AT&L))
  - Installation and Environment
- United States Transportation Command (USTRANSCOM)
- The Defense Contract Management Agency (DCMA)
  - Industrial Analysis Center
- The Defense Threat Reduction Agency (DTRA)
- The Naval Surface Warfare Center Dahlgren Division (NSWCDD)
  - Mission Assurance Division

Recommended changes or inclusions for this document can be e-mailed with the subject line "Infrastructure Resiliency Guide" to:

rss.dcipoffice@osd.mil

Table of Contents

TABLE OF CONTENTS

PURPOSE 3
INPUT ACKNOWLEDGEMENTS 4
TABLE OF CONTENTS.....6
WHAT IS DCIP?.....8
WHAT DOES DCIP DO?.....9
WHAT DOES DCIP PROVIDE? 10
OVERVIEW 11
INFRASTRUCTURES
- AVIATION TRANSPORTATION.....13
- CHEMICALS 17
- COMMUNICATIONS.....21
- ELECTRIC POWER 25
- HEATING, VENTILATION,& AIR CONDITIONING (HVAC).....29
- MARITIME TRANSPORTATION 33
- NATURAL GAS 37
- PETROLEUM 41
- RAIL TRANSPORTATION 45
- ROAD TRANSPORTATION.....50
- SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) SYSTEMS 54
- WASTE DISPOSAL 57
- WATER SYSTEMS 61

APPENDIX A - ACRONYMS 65

What is DCIP?

WHAT IS DCIP?

DCIP is a DoD risk management program designed to confirm the availability of resources deemed essential to the successful completion of DoD missions. DCIP activities include the identification, review, and analysis of assets necessary for executing the National Military Strategy.

DCIP includes both DoD and non-DoD domestic and foreign assets (e.g., defense contractors or foreign commercial support services such as telecommunications, electricity, etc.) that are essential to planning, mobilizing, deploying, executing, and sustaining U.S. military operations worldwide.

DCIP risk management involves taking actions to prevent, correct, or minimize the risks associated with vulnerabilities identified from the most important assets (i.e., Defense Critical Assets (DCAs)) that support DoD missions.

Depending on the risk, the following actions may be applied or performed on assets:

- Changes in tactics, techniques and procedures
- Adding redundancy
- Identification of an alternate capability or asset
- Isolation or hardening
- Physical protection

The goal is to reduce or eliminate unacceptable risk to DCAs, thus enabling the successful execution of DoD missions, regardless of the threat or hazard.

WHAT DOES DCIP DO?

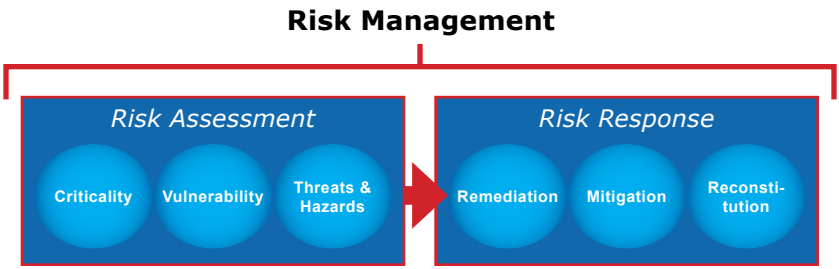
DCIP establishes the framework and the collection of information to support Risk Management of DCAs.

DCIP enables management of risk through risk assessment which:

- Establishes criticality of assets (i.e., what assets are critical in that if unavailable would cause mission degradation, disruption or failure?)
- Assesses vulnerabilities of assets (i.e., are these DCAs vulnerable, and if so, to what?)
- Identifies threats and hazards (i.e., what are the most likely things that could exploit identified vulnerabilities?)

Decision-makers then use the results of the risk assessment to determine appropriate Risk Response measures:

- Corrects or eliminates identified vulnerabilities (i.e., Remediation)
- Minimizes the impact of a potential threat or hazard (i.e., Mitigation)
- Restores lost capability in the aftermath of an event (i.e., Reconstitution)



WHAT DOES DCIP PROVIDE?

Information

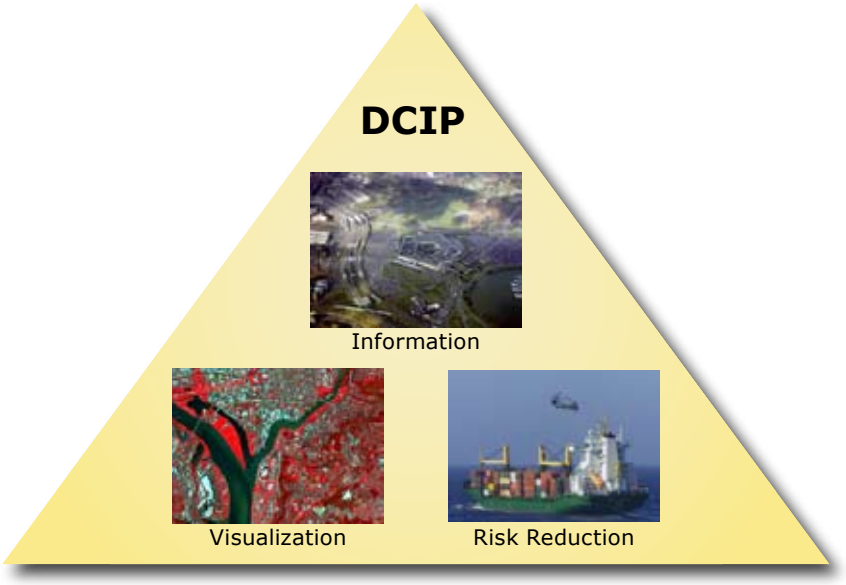
DCIP provides DoD leadership with timely and comprehensive information to make decisions to reduce the potential impact on DCAs from all threats and hazards.

Information Visualization

DCIP facilitates data and information-sharing by presenting it in an easily understood format (i.e., imagery and maps) that support risk management and resource decisions for remediation and mitigation.

Risk Reduction

DCIP provides the means for DoD leadership to know what is critical, thus allowing them to address vulnerabilities, implement continuity of operations plans, and respond to incidents with appropriate resources.



OVERVIEW

This document describes common practices that if implemented furthers reliability of the infrastructure networks DoD relies on to execute its mission. The guide is organized by infrastructure type and includes:

- Aviation Transportation
- Chemicals
- Communications
- Electric Power
- Heating, Ventilation, and Air Conditioning (HVAC)
- Maritime Transportation
- Natural Gas
- Petroleum
- Rail Transportation
- Road Transportation
- Supervisory Control and Data Acquisition (SCADA) Systems
- Waste Disposal
- Water Systems

Aviation Transportation

AVIATION TRANSPORTATION

INTRODUCTION

The U.S. military has the unique capability to move large amounts of personnel and materials by air to just about any location in the world. The civilian commercial industry also relies heavily on air travel for the delivery of materiel and goods important to their economic well being. The risks imposed by the reliance on aviation by both the military and commercial industries can be reduced by understanding dependencies, analyzing effects, and taking action.

This section provides guidelines to government and private-sector decision makers, as well as those responsible for aviation transportation, to ensure aviation disruptions do not adversely or unexpectedly affect mission accomplishment. It also includes some common vulnerabilities observed by trained assessors and multiple means of remediation for each.

GUIDELINES

Understand the mission impact of aviation transportation interruptions. Understand the aviation support requirements - what is required, when is it needed, and how it will be performed.

- Maintain current documentation of the site's aviation transportation system components (e.g., timetables, blueprints, etc.).
- Define the mission requirements for aviation transportation, to include:
  - *Timelines*
  - *Cargo types*
  - *Cargo quantities*
  - *Destinations*
- Improve aviation support resiliency by:
  - *Ensuring that the appropriate Memorandums of Agreement (MOAs) or contracts, including emergency provisions, are in place to support mission accomplishment.*
  - *Ensuring aircraft refueling capabilities are sufficient for mission accomplishment.*
  - *Ensuring Navigational Aids (NAVAIDS) are sufficient for the mission, properly maintained, and can operate in a power outage.*
  - *Identifying alternate aviation transportation facilities.*
- Ensure the necessary command and control capabilities and redundancy to monitor aviation transportation are available.
- Ensure there are sufficiently trained personnel to operate key aviation components.
- Prioritize cargoes to ensure the most critical are moved when needed.

Ensure necessary cargo-handling capability is available. Analyze the facilities, equipment, and personnel required to load/unload cargo at each destination.

- Guarantee cargo-handling capabilities are sufficient to meet mission requirements, to include:
  - *Ensuring air terminals are*

capable of processing the necessary number of passengers.

- *Ensuring the proper number and type of materiel-handling equipment (MHE) is available based on mission needs.*
- *Ensuring all identified airfields have the necessary aircraft-servicing capabilities, lighting, deicing and repair capabilities, and intermodal facilities to meet mission requirements.*
- *If required, ensuring hazardous material (HAZMAT) transportation requirements are in place.*

- Identifying backup cargo-handling capabilities.

Ensure the backup power needs of the aviation transportation elements are planned for.

Consider if a loss of power would stop nighttime air operations.

- Ensure critical aviation components that rely on electric power have backup generators.
- Ensure critical aviation assets that cannot afford power interruption have an assigned uninterruptible power supply (UPS).
- Ensure backup power systems are capable of fully supporting the aviation operations.

Maintain awareness of the safety and security of the aviation transportation system.

Limit intentional or accidental disruptions from causing mission degradation.

- Ensure HAZMAT safety requirements for aviation transportation are met.
- Ensure adequate firefighting and emergency first-responder capability.
  - *Ensure the key components of the site's aviation transportation network are provided sufficient security and monitoring, including proper lighting, locks, access controls, surveillance cameras, and motion sensors.*
- Determine the adequacy of the security level of the commercial air transportation system:
  - *Ensure commercial carriers track the contents of containers.*
  - *Ensure Defense materiel and equipment is segregated from regular commercial traffic with sufficient standoff distance.*
  - *Ensure aircraft and cargoes are secure at intermediate stops.*
  - *Ensure access control measures are in place to protect cargo.*
  - *Ensure security personnel can respond to mission locations in a reasonable amount of time.*
  - *Ensure the commercial provider has access to explosive ordnance disposal (EOD) capability.*
- Determine if commercial air facilities used outside the U.S. provide segregation of U.S. cargo from other nations. If impractical, provide a security assessment of the threat and impact of operations at this location.
- Coordinate air transportation security requirements with all appropriate parties.

Be cognizant of aviation monitoring and control system vulnerabilities.

These systems, sometimes known as SCADA systems, are used to manage and control aspects of the aviation transportation system (e.g., cargo movements). If your aviation system relies on a monitoring and control system, refer to the SCADA section in this Guidebook.

Keep aviation systems properly maintained. Plan maintenance disruptions around mission requirements.

- Ensure vulnerabilities of aviation system components are:
  - *Reviewed regularly*
  - *Remediated or mitigated as appropriate*
- Ensure the key components of the aviation system are regularly inspected, tested, and the recommended preventive maintenance is performed.
- Ensure the site has sufficient personnel and supply inventories for maintenance and emergency repair.

Implement aviation transportation contingency planning. Seek solutions to potential issues before they become problems.

- Develop contingency plans for aviation system outages. Consider other transportation means such as maritime, road, or rail.
- Ensure personnel are trained, equipped, and readily available to implement these plans.
- Exercise plans at least annually.
- Ensure plans consider the prioritization of cargoes used to support critical missions.

COMMON VULNERABILITIES

MHE is insufficient for mission needs. MHE is designed for alternative types of aircraft and is insufficient for expected cargo weight.

- Document mission requirements and resource accordingly.
- Coordinate with aviation system owners for appropriate aircraft types.
- Contract for appropriate MHE with local owners/operators.

Cargoes are insufficiently managed. Lower priority cargoes are moved out of order and site has no established means to track its delivery.

- Create movement plan based on mission requirements and timelines.
- Implement a flight-following method to track cargo delivery.

Interdependencies of the aviation system not properly identified. Site installed backup generators for NAVAIDs but did not account for the needs of electric forklifts.

- Ensure losing other supporting infrastructures does not impact aviation support.
- Seek backup solutions to identified electric power reliance through appropriate section of this guidebook.

Due to long-term maintenance, site had only one available runway. Damage or maintenance of this single point of failure (SPF) would cause mission degradation or loss.

- Implement long-term maintenance in phases to allow for quick restoration of secondary runway.
- Coordinate alternate locations to conduct transportation operations.
- Consider alternate transportation methods for contingencies (e.g., maritime, rail, or road).

Chemicals

CHEMICALS

INTRODUCTION

DoD requires chemical products to accomplish its assigned missions while the Defense Industrial Base (DIB) cannot produce many of the advanced technological weapons and systems without necessary supplies of key chemicals. The risks imposed by the reliance on chemicals by both the military and commercial industries can be reduced by understanding dependencies, analyzing effects, and taking action.

This section provides guidelines to government and private-sector decision makers, as well as those responsible for chemical support, to ensure chemical supply disruptions do not adversely or unexpectedly affect mission accomplishment. It also includes some common vulnerabilities observed by trained assessors and multiple means of remediation for each.

GUIDELINES

Understand the effects chemical supply interruptions have on mission performance. Understand the chemical product needs – what is required, when is it needed, how will it be performed.

- If supplied via pipelines, maintain current diagrams of the site's chemical support systems.
- Determine the mission-related chemical supply requirements and timelines.
- Improve chemical supply resiliency through:
  - *Establishing priority support, emergency provisions, and priority restoration contracts with suppliers (based on cost-benefit analysis).*
  - *Ensuring suppliers maintain sufficient stockpiles or have alternate sources of supply.*
- Ensure chemical supply means have redundancy, are physically diverse, and geographically separated to the maximum extent possible.
- Work with suppliers to remedy SPFs.

Establish backup supply sources. Prevent supplier problems from impacting the mission.

- Establish relationships with alternate chemical suppliers for support in an emergency.
- Maintain sufficient supplies of each required chemical product for mission execution or likely timeframe for restoration of supply disruptions.
- Identify alternate chemical options. Establish emergency sources/providers for these.

Be cognizant of chemical distribution monitoring and control system vulnerabilities. These systems, sometimes known as SCADA systems, are used to manage and control chemical distribution networks. SCADA system access can introduce risk to the chemical supply system. If your chemical distribution system has a monitoring and control system, refer to the SCADA section in this Guidebook.

Keep the chemical distribution systems properly maintained. Chemical leaks create a safety hazard as well as an interruption to mission accomplishment.

- Ensure vulnerabilities of system components are:
  - *Reviewed regularly*
  - *Remediated or mitigated as appropriate*
- Ensure the key components of the chemical distribution system are regularly inspected, tested, and the recommended preventive maintenance is performed.
- Ensure the site has sufficient personnel and supply inventories for maintenance and emergency repair.
- Ensure maintainers practice safe operating procedures, such as grounding and bonding, when working on chemical distribution infrastructure.

Ensure proper chemical distribution network safety and security. Prevent unauthorized or accidental disruptions that may impact the mission.

- Ensure the necessary Material Safety Data Sheets are properly maintained.
- Ensure local emergency response agencies are informed of the chemical types and quantities on hand.
- Ensure the proximity of chemical supplies and their potential mixing results have been considered prior to storing.
- Establish detection means for chemical spills.
- Ensure the proximity of chemical storage locations take into account the release vectors in an emergency.
- Ensure the key components of the site's chemical supply network are provided sufficient security and monitoring to include proper lighting, locks, access controls, surveillance cameras, and motion sensors.
- Determine if attempts to tamper with the chemical distribution system would be detected.
- Ensure quantities of dangerous chemicals and chemical products are accurately tracked to prevent theft.

Develop chemical distribution contingency plans. Establish mitigation for interruptions of chemical supplies.

- Ensure the site has current contingency plans in place for loss of each required chemical product supply.
- Create contingencies for interruption of chemical distribution system SPFs such as:
  - *Immediate restoration of the system*
  - *Alternative supply means*
- Ensure personnel are trained, equipped, and readily available to implement these plans.
- Exercise plans at least annually.
- Ensure plans consider the prioritization of chemical products to support critical missions.

COMMON VULNERABILITIES

The site's inventory of chemical supplies is inaccurate. Though stores could be accounted for through tracking sheets,

the inventory record did not accurately reflect the current inventories.

- Properly track chemical inventories.
- Ensure minimum requirements are identified for mission execution to allow for immediate resupply.

Chemical mixing results not properly considered for storage. Site placed focus on fire protection rather than potential spillage effects.

- Work with experienced first responders and experts to establish effective chemical storage plans.
- Determine if less toxic conditions can be achieved by using alternate types of chemicals.
- Segregate supplies to the maximum extent possible to prevent mixing.

Chemical X supplied via a single pipeline. This creates multiple SPFs in supplying this chemical.

- Install a second pipeline.
- Establish an alternate supply means (e.g., trucks).
- Maintain sufficient storage at the end-user location.
- Maintain emergency restoration capability for the pipeline.

First responders were not cognizant of chemical inventories at site. This presents both a danger to the first responders as well as a potential for not having the proper class of fire fighting equipment.

- Ensure first responders are properly informed of supply inventories.
- Ensure changes to supply inventories are immediately relayed.

The chemical supply on hand is insufficient for mission activities. The regular supplier has had numerous supply interruptions in the past two-years.

- Maintain sufficient stockpiles of necessary chemicals to ensure mission activities.
- Identify alternate suppliers.
- Identify alternative chemical for mission activities.

Communications

COMMUNICATIONS

INTRODUCTION

No supporting infrastructure better demonstrates a modern nation than its ability to effectively communicate. The risks imposed by the reliance on communication systems by both the military and commercial industries can be reduced by understanding dependencies, analyzing effects, and taking action.

This section provides guidelines to government and private-sector decision makers, as well as those responsible for communications support, to ensure communication disruptions do not adversely or unexpectedly affect mission accomplishment. It also includes some common vulnerabilities observed by trained assessors and multiple means of remediation for each.

GUIDELINES

Understand the mission impact of communication system disruptions. Understand the communication requirements – what is required, when it is needed, how it will be performed.

- Maintain current documentation of the site's communication systems architecture.
- Regularly audit mission-based communication requirements. Determine:
  - *Security requirements*
  - *Voice and data requirements*
  - *Future bandwidth requirements*
  - *Adequate bandwidth for surge conditions*
- Ensure current backup software for critical communications systems are maintained on and off site.
- Ensure all communications systems/networks are traced from point of reception/transmission back to hub to identify all SPFs.
- Work with communication service providers to add redundancy at key critical infrastructure facilities as needed.
- Ensure key communication systems resiliency through:
  - *Ensuring there are backup systems available.*
  - *Ensuring diversity of network element components.*
  - *Ensuring geographic separation of primary and alternate transmission medium.*
  - *Maintaining 'hot spares' for critical communication systems.*
- Work with commercial suppliers to remediate communication SPFs.

Identify cyber vulnerabilities in communication systems. Modern electronics are far more susceptible to monitoring and interference.

- Ensure a cyber vulnerability assessment is performed on each key communication system.
- Remediate and/or develop a contingency plan for each identified cyber vulnerability.

Be cognizant of communication systems monitoring and control system vulnerabilities. These systems, sometimes known as

SCADA systems, are used to manage and control communication networks. SCADA system access can introduce risk to the communication system. If your communication system has a monitoring and control system, refer to the SCADA section in this Guidebook.

Ensure backup power is available for critical communication systems. Do not allow a power outage to interrupt communications.

- Ensure critical communication systems have backup generators.
- Ensure communication systems that cannot afford power interruptions have an assigned UPS.
- Ensure backup systems are capable of supporting communication needs for the duration of the mission timeline.

Keep key communication system properly maintained. Plan maintenance disruptions around mission requirements.

- Ensure vulnerabilities of communication system components are:
  - *Reviewed regularly*
  - *Remediated or mitigated as appropriate*
- Ensure all communications software installed has current patches or required upgrades.
- Ensure critical components of the site's communication systems are regularly inspected, tested, and the recommended preventive maintenance is performed.
- Ensure an adequate inventory of supplies and trained personnel for routine maintenance and emergency repair.

Ensure proper communication system safety and security. Prevent accidental or deliberate communication system failures.

- Ensure maintenance on key communication systems comply with all safety requirements (e.g., grounding).
- Ensure the key components of the site's communication systems are provided sufficient security, monitoring and layers of defense.
- Establish a means to detect attempts to tamper with key communication systems.
- Ensure password protections are implemented regularly.
- Install appropriate spyware software and security patches.
- Report all suspected intrusions of communication systems to proper site authorities.

Implement communication contingency planning. Develop and verify through testing alternative means of communicating.

- Ensure the site has current contingency plans in place for interruption or loss of each key communication system.
- Ensure personnel are trained, equipped, and readily available to implement these plans.
- Exercise plans at least annually.
- Ensure plans consider prioritization to support critical mission activities.

COMMON VULNERABILITIES

Building X is an SPF for all mission critical communications. Both primary and backup systems funnel through the

same location.

- Geographically separate the primary from the alternate communications system.
- Increase security on this location during higher threat periods.

Communication network X is vulnerable due to lack of cyber defense. Information Assurance (IA) practices not fully complied with.

- Implement all required IA practices.
- Maintain required current software versions to restore capabilities.
- Establish Information Operations Condition (INFOCON) measures for increased threats.
- Utilize intrusion detection systems (IDS) on key communications networks.

Server room has a wet sprinkler system. Fire or accidental activation of the sprinkler system will destroy vital communications equipment.

- Turn off sprinkler systems in server room.
- Install a people safe dry-agent fire suppression system.
- Maintain a geographically separate and redundant server system.

The telephone exchange has no IDS or electronic monitoring capability. Lack of security increases risk to mission.

- Increase patrols and perimeter checks of facility.
- Assign security forces during events or increased threats.

Site has remote dial in capability to perform diagnosis and maintenance of communication systems. System is also not certified nor accredited.

- Establish tight security controls on this access.
- Install protective safeguards to limit ability of callers to disrupt vital communications systems.
- Certify and accredit system.

Critical mission communication requirements not fully understood and planned for. Key facilities are not identified and vital systems have backup power but their HVAC support does not.

- Identify all mission-critical communications needs and their supporting facilities.
- Ensure contingency planning for communication systems includes interdependencies on other infrastructures (e.g., electricity, HVAC).

Electric Power

ELECTRIC POWER

INTRODUCTION

The U.S. benefits from one of the most reliable electric power distribution networks in the world. However, the electric power network is a complex system of interconnected components that can fail and cause massive service disruptions. The risk and impact of electrical power failure can be reduced by understanding the dependencies, analyzing effects, and taking action.

This section provides guidelines to government and private-sector decision makers, as well as those responsible for electric power supply, to ensure electric power disruptions do not adversely or unexpectedly affect mission accomplishment. It also includes some common vulnerabilities observed by trained assessors and multiple means of remediation for each.

GUIDELINES

Understand the effect electrical power disruptions have on mission performance. Understand the requirements for electric power, how it is delivered, and the relative priority for restoring power.

- Maintain current diagrams of the electric power system.
- Ensure and maintain provider awareness of critical times when power is essential to mission execution.
- Ensure increased electrical power resiliency through:
  - *Redundant electric power feeds*
  - *Supportable electric power looped circuits*
  - *Emergency backup sources capable of sustaining mission load requirements*
- Ensure network pathways and redundancies are physically diverse and geographically separate to the greatest extent possible.
- Work with the electric power providers to identify remedies to potential single points of failure.

Keep the electric power system properly maintained. Normal wear and tear can cause service disruption if the network is not properly maintained.

- Ensure vulnerabilities of the electric power system components are:
  - *Reviewed regularly*
  - *Remediated or mitigated as appropriate*
- Retain a sufficient number of properly trained personnel to operate and maintain the system, taking into consideration normal and emergency situations.
- Ensure the key components of the electric power system are regularly inspected, tested, and the recommended preventive maintenance is performed.
- Ensure an adequate supply inventory for routine maintenance and emergency repair.

Be cognizant of electric power monitoring and control system vulnerabilities. These systems, sometimes known as SCADA systems, are used to manage

and control electric power networks. SCADA system access can introduce risk to the electrical power system. If your electric power system has a monitoring and control system, refer to the SCADA section in this Guidebook.

Maintain electric power system security. Electrical power disruptions can result in mission failure.

- Ensure the key components of the site's electric power system are provided sufficient security and monitoring (e.g., proper lighting, locks, gates, surveillance cameras, motion sensors).
- Establish a means to detect attempts to tamper with the electric power system.

Where appropriate, establish alternate power sources. In cases where unexpected, abrupt power disruption is unacceptable, evaluate the requirements for uninterrupted power supplies and generators.

- Consider the requirements for dedicated, permanently installed versus shared portable generators.
- Install an UPS for continuous flow of clean power to allow graceful shut down or transition to generators.
- Ensure adequate load capacity of the emergency equipment.
- Determine if systems require an auto-start capability. If not, establish procedures for manual transition to alternate power supplies.
- Test systems under load monthly.

Implement contingency planning. Good planning is the key to preventing disruption.

- Develop contingency plans for electrical power disruptions.
- Ensure personnel are trained, equipped, and readily available to implement the plans.
- Exercise the plans at least annually.
- Consider load shedding to support the highest priority service requirements are maintained.

COMMON VULNERABILITIES

Primary and backup electric power equipment is maintained in the same room. Though collocation of equipment may be convenient for maintenance, having both systems in the same room subjects them to the same physical threats.

- Implement physical diversity in backup support.
- Ensure fire suppression systems support continued operation of non-affected systems.
- Increase security (e.g., guard) on the location during higher threat periods.

One transformer provides both commercial and backup power to a critical asset. Alternate paths converge at a single component presenting a potential SPF. If the single common component fails, electrical service is lost.

- Where possible have independent commercial and backup power paths.

- Identify an alternate location to relocate critical operations.
- Arrange for portable generators and UPSs to supply the required power in the event of the single component failure.
- Arrange for immediate emergency maintenance response to restore the component capability.

Critical electric power assets had no access controls. Buildings that supply power to critical assets were accessible.

- Establish strict access control procedures for buildings and areas housing important system components.
- Relocate important system components to appropriately secured areas.
- Bury electric power lines or protect poles with anti-ram barriers.

Power lines share right-of-way with other key utilities. Bridges, tunnels, and trenches are often shared right-of-ways increasing their target value as well as risk.

- Establish mitigation options (e.g., backup power, transferring mission to another location, etc.) based on loss of the right-of-way.
- Establish agreements with local community to increase security or patrols for these locations during increased threat periods.
- Be cognizant of maintenance or repair activities for other utilities in these locations.

Backup generation is insufficient. Generators and UPSs are not large enough to support critical asset needs or the location does not stockpile sufficient fuel to support the operational timeframe.

- Determine critical assets needs and purchase backups accordingly.
- Maintain at least minimum operational requirements for consumables.
- Distribute critical asset operations to other backup power supplied locations.

Heating, Ventilation, & Air Conditioning

HEATING, VENTILATION, & AIR CONDITIONING (HVAC)

INTRODUCTION

HVAC needs are often overlooked for Continuity of Operations Planning even though analysis shows these systems are vital to mission accomplishment. For example, the U.S. supplies of many key medicines, such as vaccines and anti-virals require that they be maintained within a very narrow temperature range. The risks imposed by the reliance on HVAC by both the military and commercial industries can be reduced by understanding dependencies, analyzing effects, and taking action.

This section provides guidelines to government and private-sector decision makers, as well as those responsible for HVAC support, to ensure HVAC disruptions do not adversely or unexpectedly affect mission accomplishment. It also includes some common vulnerabilities observed by trained assessors and multiple means of remediation for each.

GUIDELINES

Understand the mission impact of HVAC disruptions. Understand the HVAC requirements – what is required, when it is needed, how it will be provided.

- Maintain current documentation of the site's HVAC systems.
- Define and regularly review HVAC requirements needed for mission accomplishment and HVAC modernization plans.
- Identify each supported asset's specific HVAC seasonal needs. Ensure the system:
  - *Can perform for the required duration.*
  - *Has the necessary reserve capacity to allow for maintenance or failure.*
  - *Can continue in the event of loss of commercial power or primary water supply.*
- Ensure HVAC components have physical diversity and geographic separation.

Install proper contamination controls. Limit HVAC systems from increasing mission assurance risks.

- Ensure HVAC systems have proper filtering and contamination controls.
- Ensure systems:
  - *Can automatically shut down if contamination is detected –or-*
  - *Have appropriate procedures established and annually practiced to shut down manually if contamination is detected.*
- Ensure emergency communications exist to notify all building personnel of possible contamination and required response actions.
- To the extent possible, keep reception areas (e.g., mail rooms, shipping and receiving areas, and loading docks) separate from distribution systems (e.g., utility rooms, air intakes, water, cooling, and heating mains) to confine potential contamination areas.

Be cognizant of HVAC monitoring and control system

vulnerabilities. These systems, sometimes known as SCADA systems, are used to manage and control HVAC networks. SCADA system access can introduce risk to the HVAC system. If your HVAC system has a monitoring and control system, refer to the SCADA section in this Guidebook.

Ensure necessary backup power to HVAC systems. Power outages should not stop mission accomplishment.

- Ensure HVAC systems have backup power sources.
- Ensure HVAC assets that cannot afford power interruption have an assigned UPS.
- Ensure backup power systems are capable of supporting the HVAC needs for duration of mission.

Keep HVAC systems properly maintained. Plan maintenance disruptions around mission requirements.

- Ensure HVAC key components are regularly inspected, tested, and the recommended preventive maintenance is performed.
- Ensure an adequate inventory of supplies for routine maintenance and emergency repair.

Ensure proper HVAC system safety and security. Seek to prevent accidental or deliberate HVAC system failures.

- Ensure maintenance on HVAC systems is performed in accordance with appropriate safety and HAZMAT requirements.
- Ensure the key components of the site's HVAC system are provided sufficient security and monitoring to include proper lighting, locks, access controls, surveillance cameras, motion sensors.
- Ensure the HVAC systems are designed and protected in accordance with anti-terrorism standards.

Implement HVAC contingency planning. Develop site responses for potential HVAC failures to prevent mission failure.

- Ensure the site has current contingency plans in place for interruption or loss of each required HVAC system.
- Ensure personnel are trained, equipped, and readily available to implement these plans.
- Exercise plans at least annually.
- Ensure plans consider HVAC prioritization to support critical mission activities.

COMMON VULNERABILITIES

Critical HVAC cooling components are collocated creating an SPF. This often occurs as a cost saving measure to prevent running additional power or water lines.

- Develop contingency plans for providing temporary chillers to critical assets.
- Increase security actions around these components during higher threat situations.
- Separate primary and alternate cooling components.

Shelter in place plans throughout the site do not include

procedures for securing HVAC equipment. This creates potential health risks to personnel and compromises the shelter in the event of a fire or toxic cloud situation.

- Ensure contingency plans address shutting down HVAC systems in an emergency.
- Exercise these procedures at least annually.

Critical HVAC air handling and cooling components are collocated within the mechanical room. A fire in this room will disperse smoke throughout the entire complex.

- Establish automatic shut-offs for HVAC systems in the event of a fire.
- Provide backup cooling capabilities for critical components.

Continuity of Operations (COOP) site did not consider HVAC requirements for relocated equipment. Mission requirements were considered with no thought given to supporting infrastructure.

- Ensure COOP locations meet mission needs.
- Identify alternate COOP location with sufficient additional HVAC capability.
- Install additional HVAC capability.

Air intakes do not meet anti-terrorism (AT) standards. Critical facility has an easy access point for introduction of a chemical/biological agent.

- Install the proper chem/bio protective filters.
- Modify the air intake placement to meet AT standards.
- Provide additional security during increased threats.

Maritime Transportation

MARITIME TRANSPORTATION

INTRODUCTION

Reliance upon maritime transportation for the movement of troops and supplies is vital to all large-scale military involvements. Understanding the dependencies, analyzing effects, and taking action can reduce the risk and impact of maritime transportation interruption.

This section provides guidelines to government and private-sector decision makers, as well as those responsible for maritime transportation, to ensure maritime disruptions do not adversely or unexpectedly affect mission accomplishment. It also includes some common vulnerabilities observed by trained assessors and multiple means of remediation for each.

GUIDELINES

Know how maritime operations are vital to your mission. Understand the maritime support requirements - what is required, when it is needed, and how it will be performed.

- Maintain current nautical charts of the primary and alternate waterways and services offered by the supporting facilities.
- Define the mission requirements for maritime transportation to include:
  - *Timelines*
  - *Cargo types*
  - *Cargo quantities*
  - *Destinations*
- Ensure the mission impact of all waterway restrictions, canals, chokepoints, and bridges along the mission routes are known and properly planned for.
- Ensure that the appropriate contracts for sea movement, including emergency provisions, are in place to support mission accomplishment.
- Ensure the necessary command and control capabilities for waterway transportation are available and required redundancy in place.
- Ensure there are properly trained and sufficient personnel to operate and maintain key maritime components (cranes, locks, etc.).
- Prioritize cargo loading to ensure the most critically needed are moved when required.

Ensure necessary cargo handling capability is available. This includes the facilities, equipment, and personnel required to load/unload cargo at each destination.

- Ensure cargo handling capabilities are sufficient to meet mission requirements to include:
  - *Ensuring all identified facilities have the necessary services, facilities, materiel handling equipment, and repair capabilities.*
  - *Ensuring the proper number and type of materiel handling equipment is available based on mission needs.*
  - *Ensuring port facilities are capable of meeting mission requirements for loading, unloading, capacity, and surging.*
  - *Ensuring sufficient backup power is available.*

- *If required, ensuring HAZMAT transportation requirements are in place.*

- Identify backup cargo handling capabilities.

Keep safety and security in the forefront of maritime operations. Prevent disruptions from causing mission failure or degradation.

- Ensure HAZMAT safety requirements for waterway transportation are met.
- Work with the Coast Guard during loadouts to:
  - *Limit vessel traffic.*
  - *Track all vessels.*
  - *Perform random boarding of vessels.*
- Ensure adequate firefighting and emergency first responder capability.
- Ensure the ports and piers have sufficient lighting for safe and secure operations.
- Work with the Federal Aviation Administration to establish no-fly zones over military loadouts.
- Determine the adequacy of the security level of the ports and piers:
  - *Ensure port officials know the contents of containers and investigate discrepancies.*
  - *Ensure defense materiel and equipment segregated from regular port traffic with sufficient standoff distance.*
  - *Ensure access control measures in place for protecting cargo.*
  - *Ensure site security personnel can respond to critical mission locations in a reasonable amount of time.*
  - *Ensure additional security is available during increased Homeland Security or Maritime Security threat levels.*
  - *Ensure the site has ready access to an EOD capability.*
- Ensure essential ports outside the U.S. provide separation of U.S. ships and cargo from foreign ships. If impractical, provide a security assessment and required protections for the U.S. operations at that location.

Develop contingency plans for those critical aspects of maritime operations. Determine appropriate responses before the situation demands them.

- Prioritize maritime cargo to ensure the most efficient movement in support of your mission.
- Determine if the Captain of the Port has a Port Security Committee that maintains port contingency plans.
- Identify alternate shipping facilities and methods if the primary system is disrupted.
- Ensure these plans are exercised at least annually.

Ensure proper maritime system maintenance and repair. Prevent costly disruptions before they occur.

- Ensure the waterways are properly maintained (dredged, marked, protected from shoaling, etc.).
- Enter into private salvage contracts to clear shipping channels in an emergency.
- Ensure the key components of the waterway transportation system are regularly inspected, tested, and the recommended preventive maintenance is performed.

- Ensure the site has sufficient maintenance personnel and supply inventories.
- Ensure vulnerabilities of maritime system components are:
  - *Reviewed regularly*
  - *Remediated or mitigated as appropriate*

COMMON VULNERABILITIES

Port cranes were not currently operational or certified. Mission requirements make access to these essential.

- Keep vital equipment serviced and operational.
- Ensure critical maritime assets are available before beginning operations at this location. Plan for and use contingency alternatives.
- Ensure those facilities outside your control have proper maintenance and repair programs in place.

There is limited explosive detection equipment at the port. Defense cargoes are stored in close proximity to civilian and foreign loads.

- Use facilities that implement or have access to explosive detection equipment.
- Ensure appropriate standoff distances or barriers separate your cargo from others.
- Move cargo directly aboard ship to avoid storage concerns.

Water depths at some key piers and turning basins are too shallow for the majority of ships that need to use these facilities during an operation. Port operators were unaware of contingency plans to use these facilities.

- Pursue deeper dredging options with the appropriate port authorities.
- Ensure sounding data is kept up to date.
- Use shallower draft shipping for operations in this port.
- Use alternative shipping facilities that can accommodate deeper draft vessels.

Port operations are reliant upon a critical number of key local contractor personnel. The additional risks imposed by the potential of striking workers, contract disputes, and uncleared personnel contribute to increased risk to mission accomplishment.

- Establish organic port operations capability.
- Ensure port authorities keep customers informed of potential contractor issues.
- Work with the port authorities to ensure background checks on all personnel with access to critical maritime assets or cargo.

Natural Gas

NATURAL GAS

INTRODUCTION

Natural gas and propane provide the U.S. a relatively clean alternative fuel versus traditional coal. In September 2004, natural gas prices jumped 17% in two days due to industry concerns over supply and demand. That is the equivalent of gasoline increasing nearly 50 cents a gallon in today's market prices. The risks imposed by the reliance on natural gas by both the military and commercial industries can be reduced by understanding dependencies, analyzing effects, and taking action.

This section provides guidelines to government and private-sector decision makers, as well as those responsible for natural gas supply, to ensure natural gas disruptions do not adversely or unexpectedly affect mission accomplishment. It also includes some common vulnerabilities observed by trained assessors and multiple means of remediation for each.

GUIDELINES

Understand the effects of natural gas disruptions on mission performance. Understand the natural gas requirements – what is required, when it is needed, how it is delivered.

- Maintain current diagrams of the site's natural gas system.
- Determine the mission-related natural gas requirements and timelines.
- Improve natural gas supply resiliency through:
  - *Implementing priority service and restoration contracts with the supplier (based on cost-benefit analysis).*
  - *Ensuring suppliers maintain sufficient stockpiles/storage.*
  - *Coordinating with the Defense Energy Support Center (DESC) for procuring additional supply sources.*
- Where practical, ensure natural gas supply lines have redundancy, are physically diverse, and geographically separated to the maximum extent possible.
- Work with suppliers to remedy SPFs where practical.

Identify backup supply sources. Prevent supplier disruptions from impacting mission accomplishment.

- Maintain minimum backup supplies of natural gas required to carry out operations for their entirety.
- Research and maintain alternative sources of natural gas and alternative fuels.
- Identify assets capable of using alternative products (e.g., propane) and establish sources/providers for these.

Develop natural gas contingency plans. Prepare options for interruptions of the natural gas supply.

- Develop contingency plans for service disruptions or interruption at each natural gas SPF.
- Ensure personnel are trained, equipped, and readily available to

implement these plans.

- Exercise plans at least annually.
- Ensure plans consider prioritization of natural gas in support of critical missions.

Be cognizant of natural gas monitoring and control system vulnerabilities. These systems, sometimes known as SCADA systems, are used to manage and control natural gas transmission, storage and distribution networks. SCADA system access can introduce risk to the natural gas system. If your natural gas distribution system has a monitoring and control system, refer to the SCADA section in this Guidebook.

Maintain awareness of natural gas distribution network safety and security. Prevent unauthorized or accidental disruptions that may impact the mission.

- Ensure the key components of the site's natural gas distribution network are provided sufficient security and monitoring to include proper lighting, locks, access controls, surveillance cameras, and motion sensors.
- Determine if attempts to tamper with the natural gas system would be detected.

Keep the natural gas system properly maintained. Gas leaks create a safety hazard as well as an interruption to mission accomplishment.

- Ensure vulnerabilities of the natural gas distribution system components are:
  - *Reviewed regularly*
  - *Remediated or mitigated as appropriate*
- Ensure the key components of the natural gas distribution system are regularly inspected, tested, and the recommended preventive maintenance is performed.
- Ensure an adequate supply inventory and properly trained personnel for routine maintenance and emergency repair.

COMMON VULNERABILITIES

The natural gas supply manifold collocated with electrical power, HVAC components and a mission critical asset. Catastrophic failure of the electrical power or HVAC systems could destroy the natural gas manifold and the critical asset.

- Move the critical asset to a more protected location.
- Install explosive protections around the natural gas manifold and the critical asset.
- Move HVAC and electric power components.

The natural gas supply to the site arrives via a single feed underneath a bridge. Destruction of the bridge or maintenance issues may interrupt natural gas supplies, preventing mission accomplishment.

- Establish on site a separate location for storage of natural gas or an alternative fuel with sufficient quantities capable of sustaining critical missions.
- Develop contingency plans in concert with natural gas suppliers and the DESC for natural gas/alternative fuel delivery.

- Coordinate with the pipeline owner to monitor maintenance activities on the SPF.
- Develop a MOA with the local authorities for increase bridge protection during higher threat periods.
- If practical, seek a second feed line for natural gas that is geographically separate from the primary supply line.

Fire suppression systems at natural gas supply locations are not appropriate for that type of fire. This happens when natural gas systems are collocated with electric power assets.

- Install fire suppression systems capable of each type of potential fire.
- Relocate either system to another location and ensure correct fire suppression systems available.

The site's contract has no emergency or priority restoration clauses. Site is also last on natural gas supplier's restoration list.

- Review supply contracts to ensure appropriate emergency response in relationship to criticality of mission.
- Contract with another supplier for improved responsiveness.
- Maintain appropriate supply levels on site.
- Maintain the required natural gas maintenance and repair capabilities on site.

Petroleum

PETROLEUM

INTRODUCTION

Petroleum products form the basis for many aspects of the nation's economy, from providing fuel to run engines to providing plastics and other materials from which goods are made. The risk and impact of a petroleum supply failure can be reduced by understanding the dependencies, analyzing effects, and taking action.

This section provides guidelines to government and private-sector decision makers, as well as those responsible for petroleum supply, to ensure petroleum disruptions do not adversely or unexpectedly affect mission accomplishment. It also includes some common vulnerabilities observed by trained assessors and multiple means of remediation for each.

GUIDELINES

Understand the effects interruptions of petroleum and petroleum products have on mission performance. Understand the petroleum requirements (e.g., types, quantities, how supplies are transported and handled, and where the supplies come from).

- Maintain current diagrams of the site's petroleum supply and distribution system(s).
- Determine the amount of petroleum products required for mission execution and the timelines when they are required.
- Improve petroleum supply resiliency through:
  - *Establishing priority service and restoration contracts with suppliers (based on a cost-benefit analysis).*
  - *Ensuring suppliers maintain sufficient stockpiles.*
  - *Coordinating with DESC for procuring alternative supply sources.*
  - *Coordinating with the Defense Fuel Support Points to track inventory levels.*
- Ensure petroleum distribution means have redundancy, are physically diverse, and geographically separated to the maximum extent possible.
- Analyze internal and external systems and work with suppliers to remedy SPFs.

Identify backup supply sources. Do not become reliant upon a single source.

- Research and maintain alternative sources of required petroleum products.
- To the extent possible, maintain the minimum quantity of backup supplies required to carry out operations for their entirety.
- Identify assets capable of using alternate fuels and establish sources/providers for these.

Be cognizant of petroleum supply monitoring and control system vulnerabilities. These systems, sometimes known as SCADA systems, are used to manage and control petroleum transmission, storage, and supply distribution networks. SCADA system access can introduce risk to the petroleum

supply system. If your petroleum supply distribution system has a monitoring and control system, refer to the SCADA section in this Guidebook.

Ensure proper petroleum distribution system safety and security. Petroleum supplies and storage facilities are tempting targets.

- Ensure the proper firefighting capabilities are available based on the petroleum products in use.
- Ensure the key components of the site's petroleum supply network are provided sufficient security and monitoring (e.g., proper lighting, locks, access controls, surveillance cameras, motion sensors).
- Establish a means to detect attempts to tamper with the petroleum supply and distribution system(s).

Keep petroleum distribution systems properly maintained. Prevent maintenance-related disruptions of the system.

- Ensure maintenance personnel practice safe operating procedures, such as grounding and bonding, when working on petroleum infrastructure.
- Ensure vulnerabilities of the petroleum distribution system components are:
  - *Reviewed regularly*
  - *Remediated or mitigated as appropriate*
- Ensure the key components of the petroleum distribution system are regularly inspected, tested, and the recommended preventive maintenance is performed.
- Ensure an adequate supply inventory for routine maintenance and emergency repair.

Implement petroleum distribution contingency planning. Seek solutions to potential issues before they become problems.

- Develop contingency plans for supply disruptions of each petroleum product or interruption at each SPF.
- Ensure personnel are trained, equipped, and readily available to implement these plans.
- Exercise plans at least annually.
- Ensure plans consider the prioritization of petroleum products used to support critical missions.

COMMON VULNERABILITIES

The fuel supply and distribution system has multiple single points of failure. Any of these and dependent infrastructure SPFs can stop fuel from reaching the flight line.

- Develop a fuel COOP Plan and validate it through exercises.
- Evaluate fuel truck supply feasibility.
- Increase security on exposed fuel lines, valve pits, and equipment.
- Maintain inventory of critical fuel system repair parts.

The backup generator fuel tank is collocated with an electric power transformer. This may also include other devices prone to explosions or fire.

- Move the fuel tank to a different location.
- Bury the fuel tank.

PETROLEUM (continued)

- Install proper fire and explosive protection barriers between these assets.

The bulk petroleum facility has a dial-in capability for monitoring and controlling operations remotely. Access is a potential means for hackers or former employees to interrupt supplies.

- Install cyber protections to prevent unauthorized access of the system.
- Limit the operations that can be accomplished remotely.

The petroleum storage facility lacks lightning protection. This is a potential life and death issue in addition to impacting the mission.

- Properly ground the facility.
- Bury the storage tanks.
- Implement contingency operations during inclement weather.

The petroleum storage facility lacks backup power. Loss of commercial power means loss of pumping operations.

- Install a backup generator.
- Purchase manual pumps.
- Identify an alternate refueling location in the event of power loss.

Site's contingency plan only deals with alternate suppliers of petroleum products. Plan does not take into account infrastructure interruptions.

- Ensure interruption at each SPF is planned for.
- Maintain appropriate inventories of parts and trained personnel to repair SPFs.
- Identify alternate locations to perform petroleum required operations.

Rail Transportation

RAIL TRANSPORTATION

INTRODUCTION

For movement of mass tonnage across the U.S. and many foreign countries, rail transportation still provides the most efficient means. Today, the U.S. military relies upon rail transportation especially for movement of heavy materials to cargo loading facilities at ports. The risks imposed by the reliance on rail transportations by both the military and commercial industries can be reduced by understanding dependencies, analyzing effects, and taking action.

This section provides guidelines to government and private-sector decision makers, as well as those responsible for rail transportation support, to ensure rail transportation disruptions do not adversely or unexpectedly affect mission accomplishment. It also includes some common vulnerabilities observed by trained assessors and multiple means of remediation for each.

GUIDELINES

Understand the mission impact of rail transportation interruptions. Understand the rail support requirements - what is required, when is it needed, how will it be performed.

- Maintain current maps and timetables of the primary and alternate railway transportation system.
- Define the mission requirements for rail transportation to include:
  - *Timelines*
  - *Cargo types*
  - *Cargo quantities*
  - *Destinations*
- Ensure the mission impact of all railway restrictions, tunnels, chokepoints, and bridges along the mission routes are known and properly planned for.
- Ensure that the appropriate contracts for rail movement, including emergency provisions and access to required locomotives and freight cars, are in place to support mission accomplishment.
- Ensure both the primary and alternate rail facilities have the necessary services, material handling equipment, and repair capabilities.
- Ensure the necessary command and control capabilities for railway transportation are available and required redundancy in place.
- Ensure there are properly trained and sufficient personnel to operate key railway components (intermodal facilities, switching locations, etc.)
- Prioritize cargoes to ensure most critical are moved when needed.

Ensure necessary cargo handling capability is available. Analyze the facilities, equipment, and personnel required to load/unload cargo at each destination.

- Ensure cargo handling capabilities are sufficient to meet mission requirements to include:
  - *Ensuring the proper number and type of materiel handling*

equipment is available based on mission needs.
- *Ensuring rail yards and loading facilities are capable of meeting mission requirements for loading, unloading, capacity and surging.*
- *Ensuring sufficient backup power is available.*
- *If required, ensuring HAZMAT transportation requirements are in place.*

- Identify backup cargo handling capabilities.

Ensure backup power needs of the rail transportation elements are planned for. Consider if power loss or nighttime operations would stop rail operations.

- Ensure critical railway elements reliant upon electric power have backup generators.
- Ensure critical railway assets that cannot afford power interruption have an assigned UPS.
- Ensure backup power systems are capable of fully supporting the railway operations.

Ensure proper railway system maintenance and repair. Prevent costly disruptions before they occur.

- Ensure the rail pathways are properly maintained (monitored, plowed, removal of debris performed, etc.).
- Ensure the critical and key components of the site's railway transportation system are regularly checked, tested, and the necessary preventive maintenance is performed.
- Ensure vulnerabilities of rail transportation system components are:
  - *Reviewed regularly*
  - *Remediated or mitigated as appropriate*
- Ensure the site has sufficient maintenance personnel and supply inventories.

Keep informed on the safety and security of the railway transportation system. Limit intentional or accidental disruptions from causing mission degradation.

- Ensure HAZMAT safety requirements for railway transportation are met.
- Ensure adequate firefighting and first responder capability.
- Ensure rail loading and unloading facilities have sufficient lighting for safe and secure operations.
- Determine the adequacy of security in the commercial rail transportation system:
  - *Ensure rail officials track the contents of containers and visually inspect railcars.*
  - *Ensure defense materiel and equipment segregated from regular commercial traffic with sufficient standoff distance.*
  - *Ensure commercial rail providers monitor Homeland Security and Maritime Security threat levels and respond to increases appropriately.*
  - *Ensure security enclosures around signals and switches to prevent unauthorized access to control panels.*
  - *Ensure access control measures in place to protect cargo.*
  - *Ensure security personnel respond to mission required locations in a reasonable amount of time.*
  - *Ensure the commercial provider has access to an EOD capability.*

- Patrol the movement route prior to and during rail movements.
- Establish a working relationship with the American Association of Railroads to enhance information sharing.
- Determine if commercial rail providers outside the U.S. provide segregation of U.S. cargo from other nations. If impractical, provide a security assessment of the threat and impact of operations at this location.

Develop contingency plans for those critical aspects of railway transportation. Identify appropriate responses to potential problems.

- Develop contingency plans for rail transportation disruptions. Consider other means (e.g., maritime, road, or air).
- Ensure personnel are trained, equipped, and readily available to implement these plans.
- Exercise plans at least annually.
- Ensure plans consider the prioritization of cargoes used to support critical missions.
- Determine if commercial rail providers maintain contingency plans.

COMMON VULNERABILITIES

Rail lines supporting the site have multiple SPFs. SPFs are also publicly accessible and easily disrupted.

- Identify alternate locations and routes for rail SPFs.
- Work with commercial providers to seek remedies to SPFs.
- Establish MOAs with appropriate authorities to increase security around rail SPFs during higher threats.

Commercial rail transportation provider has only a single access spur with the site. Alternate provider's lines run within ¼ mile of loading facility.

- Contract with alternate provider to extend access spur to facility.
- Contract with alternate provider for local intermodal facility.
- Identify alternative intermodal facilities for use with primary rail provider.

Mission required HAZMAT cargoes are restricted from movement through population centers. Rail lines supporting transportation from site to port must transverse these locations.

- Change plans to identify alternate delivery ports without restrictions.
- Establish Memorandums of Understanding (MOUs) with local authorities for movements through these locations in times of emergency.
- Transport HAZMAT via alternate means (road, air, etc.)

Commercial rail provider's maintenance planning is insufficient to support mission requirements. 33% of required locomotives and rail cars are unavailable due to maintenance and repair activities.

- Contract with provider to ensure necessary support available.
- Contract with alternate provider for additional support.

Rail facilities lack illumination for nighttime loading activities.

Site maintains 12 emergency light carts, but requires 26 based on site contingency plans.

- Prioritize light carts to critical mission locations.
- Purchase additional light carts.
- Purchase backup generator for rail facility lighting.

Road Transportation

ROAD TRANSPORTATION

INTRODUCTION

The U.S. relies heavily upon its road infrastructure to provide essential services, move goods to market, and foster travel. Roads are also key to national security. In foreign countries roads serve these same purposes, but unfortunately much of the world's road infrastructure lags far behind the U.S.. The risks imposed by the reliance on aviation by both the military and commercial industries can be reduced by understanding dependencies, analyzing effects, and taking action.

This section provides guidelines to government and private-sector decision makers, as well as those responsible for road transportation support, to ensure roadway disruptions do not adversely or unexpectedly affect mission accomplishment. It also includes some common vulnerabilities observed by trained assessors and multiple means of remediation for each.

GUIDELINES

Understand the mission impact of road transportation interruptions. Understand the roadway support requirements - what is required, when is it needed, how it will be performed.

- Maintain current maps of the primary and alternate travel routes for the site's road transportation requirements.
  - *Where possible, keep mission related activities separate from heavy general traffic flows.*
  - *Schedule military shipments to arrive/depart at off-peak hours.*
- Define the mission requirements for road transportation to include:
  - *Timelines*
  - *Cargo types*
  - *Cargo quantities*
  - *Destinations*
- Ensure appropriate contracts, including emergency provisions and access to necessary vehicles, are in place.
- Ensure mission impact of all roadway restrictions (e.g., bridges, tunnels) along travel routes are known and properly planned for (weight, height, width, availability, etc.).
- Ensure the necessary command and control capabilities for road transportation operations are available and required redundancy in place.

Ensure necessary cargo handling capability is available. This includes the facilities, equipment, and personnel required to load/unload cargo at each destination.

- Ensure cargo handling capabilities are sufficient to meet mission requirements to include:
  - *Ensuring loading, unloading, capacity, and surging capabilities are sufficient.*
  - *Ensuring the proper number and type of materiel handling equipment is available based on mission needs.*
  - *Ensuring servicing/ refueling capabilities are sufficient for mission needs.*

- *If required, ensuring HAZMAT transportation requirements are in place.*

- Identify backup cargo handling capabilities.

Ensure road transportation elements backup power requirements are planned for. Prevent power outages from impacting mission accomplishment.

- Ensure critical road transportation elements reliant upon electric power have backup generators.
- Ensure critical roadway assets that cannot afford power interruption have an assigned UPS.
- Ensure backup systems are capable of fully supporting roadway operations.

Ensure proper roadway transportation system maintenance and repair. Ensure elements remain available for mission needs.

- Ensure the roadway routes are properly maintained (plowed, repaired, etc.).
  - *Monitor the maintenance status of roads, bridges, tunnels, etc., along primary and secondary travel routes.*
- Ensure vulnerabilities of road transportation system components are:
  - *Reviewed regularly*
  - *Remediated or mitigated as appropriate*
- Ensure roadway transportation system elements are regularly inspected, tested, and the required preventive maintenance is performed.
- Ensure the site has sufficient maintenance personnel and supply inventories.

Keep informed on the safety and security of the roadway transportation system. Prevent accidental or intentional disruptions.

- Ensure HAZMAT safety requirements for roadway transportation are met.
- Ensure proper fire fighting and emergency first responder capability is available.
- Ensure loading and unloading facilities have sufficient lighting for safe and secure operations.
- Determine the security level of commercial road transportation providers.
  - *Ensure the commercial carrier tracks the contents of all containers.*
  - *Implement Intelligent Transportation Systems to improve safety and security.*
  - *Ensure defense materiel and equipment is segregated from regular commercial traffic with sufficient standoff.*
  - *Ensure access control measures are in place to protect cargo at all stops along travel routes.*
  - *Ensure security personnel can respond to mission required locations in a reasonable amount of time.*
  - *Ensure the commercial carrier has access to an EOD capability.*
- Patrol road transportation routes prior to and during movements.
- Determine if commercial carriers outside the U.S. provide segregation of U.S. cargo from other nations.
  - *If impractical perform a security assessment of the impact, vulnerability, and threats to operations with this carrier.*

Develop contingency plans for critical aspects of roadway transportation. Determine appropriate responses before situations demand them.

- Prioritize cargo to ensure most efficient movement in support of your mission.
- Identify alternative shipping facilities, routes, and means (e.g., rail, maritime, air) if road elements are disrupted.
- Ensure personnel are trained, equipped, and readily available to implement these plans.
- Exercise plans at least annually.
- Review commercial carrier contingency plans.

COMMON VULNERABILITIES

Site's materiel handling equipment is not properly maintained and serviced. Site is incapable of meeting loading and surge needs required by mission.

- Ensure preventive maintenance is kept up.
- Identify alternate sources of material handling.

All site transportation requires movement along a single bridge. Accidents or bridge maintenance will stop all required operations.

- Identify alternative means of transportation (e.g., rail, air or maritime) that does not rely upon this bridge.
- Monitor bridge maintenance activities.

Vehicle inspections are inadequate. Cargo container contents are not verified prior to reaching critical site locations.

- Establish procedures to check cargo in a safe location.
- Use electronic monitored tracking containers to verify content integrity.
- Install container detection systems.

Commercial cargo carriers do not segregate military cargo. U.S. cargoes stored in close proximity to other nation's cargo.

- Identify alternative carriers.
- Contract to ensure security of cargo.

The site is incapable of tracking cargo between point or origin and destination. Mission delays have occurred when vehicle breakdowns could not be properly addressed.

- Implement a command and control process to track shipping.
- Use satellite tracking containers for shipping.
- Establish procedures for notification by drivers of delays.

Supervisory Control & Data Acquisition Systems

SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) SYSTEMS

INTRODUCTION

The term SCADA generally refers to any large-scale, distributed measurement (and control) systems. SCADA systems are used to monitor and/or to control chemical or transport processes, in municipal water supply systems, to control electric power generation, transmission and distribution, gas and oil pipelines, and other distributed infrastructure processes. The risks imposed by the reliance on SCADA systems by both the military and commercial industries can be reduced by understanding dependencies, analyzing effects, and taking action.

This section provides guidelines to government and private-sector decision makers, as well as those responsible for SCADA-type systems, to ensure SCADA system disruptions do not adversely or unexpectedly affect mission accomplishment. It also includes some common vulnerabilities observed by trained assessors and multiple means of remediation for each.

GUIDELINES

Have a cyber–related threat assessment conducted on each SCADA system.

- Ensure each cyber access point is identified.
- Monitor and report attempts to hack into the system.

Ensure appropriate access control procedures are established and practiced.

- Implement appropriate identity verification and password protections for the system.
- Identify all personnel with access to the system.
- Ensure transferred personnel are removed from accessing the system.
- Ensure original system passwords are removed.
- Make risk management decisions on those critical operations that can cause system failure or damage.
- Consider only allowing them to be performed manually or after two-person verification.

Train SCADA operators to perform functions independent of SCADA systems.

- Maintain quick reference checklists to perform key SCADA functions manually.
- Ensure this capability is exercised at least annually.

Ensure SCADA systems have backup power and communications systems.

- Install backup generators and/or an UPS with sufficient capability to maintain system.
- Ensure backup communications sufficient to meet SCADA requirements.
- Ensure backup systems are tested annually at a minimum.

Ensure immediate repair capabilities for the SCADA system are available.

- Contract for immediate response for key SCADA systems.
- Ensure current SCADA backup software is maintained by the site.
- Ensure appropriately trained maintenance personnel and part inventories are available.

COMMON VULNERABILITIES

SCADA system control room is serviced by a wet sprinkler. Sprinkler failure or fire will destroy electronic portions of system.

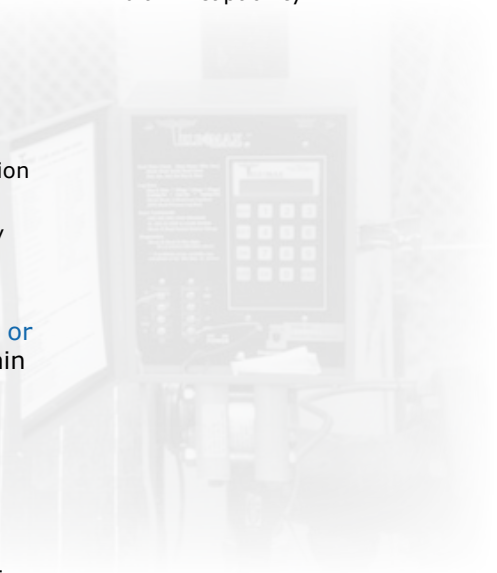
- Install dry-based fire suppression systems.
- Install 30-second manual delay cutoff, to prevent accidental water system activation.

SCADA system is not certified or accredited. System may contain unknown vulnerabilities.

- Ensure SCADA systems are approved prior to installation.
- Have a cyber-related security assessment performed on the SCADA system.
- Record and remediate all identified vulnerabilities.

Electric power SCADA system is remotely accessible on not properly secured against unauthorized intrusion. Unauthorized personnel are capable of turning power off to key locations.

- Establish access controls for SCADA systems.
- Limit/prevent critical operations from being accomplished via dial-in capability.



Waste Disposal

WASTE DISPOSAL

INTRODUCTION

For the purpose of this guide, reliance upon waste disposal systems includes all those processes that move waste from the site to its ultimate destination such as a water treatment plant or landfill. Though disruptions in these services will likely not have the immediate detrimental effect of a commercial power outage, they still pose a potential negative effect to mission operations or serve as a potential target for attack. The risks imposed by the reliance on waste disposal by both the military and commercial industries can be reduced by understanding dependencies, analyzing effects, and taking action.

This section provides guidelines to government and private-sector decision makers, as well as those responsible for waste disposal, to ensure waste disposal disruptions do not adversely or unexpectedly affect mission accomplishment. It also includes some common vulnerabilities observed by trained assessors and multiple means of remediation for each.

GUIDELINES

Understand the effect waste disposal disruptions have on mission performance. Understand the requirements for waste disposal, how it is transported, and the relative priority for restoring this service.

- Maintain current diagrams of the site's wastewater removal and HAZMAT disposal systems.
- Keep informed of critical times when waste removal is essential to mission execution. Ensure this review takes into account:
  - *New requirements.*
  - *A modernization plan to replace outdated portions of the system.*
  - *Seasonal changes/need.*
- Ensure waste disposal resiliency through:
  - *Identifying alternative disposal means/contracts.*
  - *Implementing physical diversity and geographic separation in disposal pathways.*
- Ensure the site has a waste disposal backup storage site that is sufficient to support mission timeline requirements.
- Ensure the site is able to isolate portions of the waste disposal system for prioritization to mission critical assets.
- Work with waste disposal providers to identify remedies to potential SPFs.

Be cognizant of waste disposal monitoring and control system vulnerabilities. These systems, sometimes known as SCADA systems, are used to manage and control waste disposal networks. SCADA system access can introduce risk to the waste disposal system. If your waste disposal system has a monitoring and control system, refer to the SCADA section in this Guidebook.

Ensure critical waste disposal elements backup power requirements are planned for. Prevent power outages from impacting mission accomplishment.

- Ensure critical waste disposal elements reliant upon electric power have backup generators.
- Ensure critical waste disposal assets that cannot afford power interruption have an assigned UPS.
- Ensure backup systems are capable of fully supporting waste disposal requirements.

Keep waste disposal system elements properly maintained. Normal wear and tear can be the cause of system interruptions if the network is not properly maintained.

- Ensure vulnerabilities of waste disposal system components are:
  - *Reviewed regularly*
  - *Remediated or mitigated as appropriate*
- Ensure the key components of the waste disposal systems are regularly inspected, tested, and the recommended preventive maintenance is performed.
- Retain a sufficient number of properly trained personnel to operate and maintain waste systems.
- Maintain an adequate supply inventory for routine and emergency repair.

Maintain waste disposal system safety and security. Seek to prevent accidental or intentional disruptions of these systems.

- If required by mission, ensure all appropriate HAZMAT safety, storage, and transportations requirements are complied with.
- Ensure proper firefighting and emergency first responder capability exists.
- Ensure the key components of the site's waste disposal system are provided sufficient security and monitoring to include proper lighting, locks, gates, surveillance.
- Ensure the waste disposal systems are designed and protected in accordance with anti-terrorism standards.

Implement waste disposal contingency planning. Good planning is the key to preventing disruption.

- Develop contingency plans for interruption or loss of waste disposal systems.
- Ensure personnel are trained, equipped, and readily available to implement.
- Exercise plans at least annually.
- Ensure plans consider prioritization support to critical mission activities.

COMMON VULNERABILITIES

Waste disposal site in close proximity to backup water supply source. Accidental or intentionally destructive acts have potential to contaminate needed water source.

- Relocate waste storage site to safer location.
- Increase security on this location.
- Install drainage system to prevent leakage from contaminating water sources.

WASTE DISPOSAL (continued)

Waste disposal is reliant upon commercial service provider.

Contract negotiations have caused disruptions to service at the site.

- Include priority service clauses in contracts with service providers.
- Identify alternative waste disposal service providers and contract for emergency service.

Water Systems

WATER SYSTEMS

INTRODUCTION

Water is often overlooked as a primary requirement for military operations. Most military operations that involve hazardous materials or weapons require an in-place firefighting capability. Many heating and cooling systems rely on a water supply to operate. The risks imposed by the reliance on water supplies by both the military and commercial industries can be reduced by understanding dependencies, analyzing effects, and taking action.

This section provides guidelines to government and private-sector decision makers, as well as those responsible for water distribution, to ensure water disruptions do not adversely or unexpectedly affect mission accomplishment. It also includes some common vulnerabilities observed by trained assessors and multiple means of remediation for each.

GUIDELINES

Understand the effect water distribution disruptions have on mission performance. Understand the requirements for water, how it is transported, and the relative priority for restoring this service.

- Maintain current diagrams of the site's water distribution systems.
- Ensure awareness of water requirements for mission accomplishment. Ensure this review takes into account:
  - *New requirements.*
  - *A modernization plan to replace outdated portions of the system.*
  - *Seasonal changes/needs.*
- Ensure water distribution resiliency through:
  - *Identifying alternative supply means.*
  - *Physical diversity and geographic separation in water supply pathways.*
- Ensure the site has a backup water supply that is sufficient to support mission timeline requirements.
- Ensure the site is able to isolate portions of the water distribution system to prioritize flows to mission critical assets.
- Work with water distribution providers to identify remedies to potential SPFs.

Ensure critical water distribution elements have backup power. Prevent power outages from impacting mission accomplishment.

- Ensure critical water distribution elements reliant upon electric power have backup generators.
- Ensure critical water distribution assets that cannot afford power interruption have an assigned UPS.
- Ensure backup systems are capable of fully supporting water distribution requirements.

Be cognizant of water system monitoring and control system vulnerabilities. These systems, sometimes known as SCADA systems, are used to manage and control water distribution

networks. SCADA system access can introduce risk to the water distribution system. If your water distribution system has a monitoring and control system, refer to the SCADA section in this Guidebook.

Maintain water distribution system safety and security. Ensure the water system supports, not hinders, mission accomplishment.

- Establish safe practices for water system maintenance.
- Ensure water distribution systems have filtering and contamination controls.
- Ensure the water distribution systems:
  - *Can automatically shut down if contamination is detected –or-*
  - *Procedures are in place and regularly practiced to shut down manually if contamination is detected.*
- Ensure the key components of the site's water distribution system are provided sufficient security and monitoring to include proper lighting, locks, gates, surveillance cameras, and motion sensors.
- Ensure the water distribution systems are designed and protected in accordance with anti-terrorism standards.

Keep water distribution system elements properly maintained. Normal wear and tear can be a source or mission disruption.

- Ensure vulnerabilities of water distribution system components are:
  - *Reviewed regularly*
  - *Remediated or mitigated as appropriate*
- Ensure the key components of the site's water distribution systems are regularly inspected, tested, and the recommended preventive maintenance is performed.
- Retain a sufficient number of properly trained personnel to operate and maintain water distribution systems.
- Maintain an adequate supply inventory for routine and emergency repair.

Implement water distribution contingency planning. Good planning is key to preventing disruptions.

- Develop contingency plans for interruption or loss of the water distribution systems.
- Ensure personnel are trained, equipped, and readily available to implement.
- Exercise plans at least annually.
- Implement prioritization of water distribution to critical mission activities.

COMMON VULNERABILITIES

Building X is an SPF for water delivery to the entire base. Site maintains insufficient backup storage of water to meet mission requirements.

- Establish water supply based on daily usage at site and total required for mission accomplishment.
- Implement water rationing and prioritization when required.

- Establish contingency plans for delivery of emergency water supplies from nearest available location.
- Increase security on building during heightened threat levels.

Water distribution lacks backflow prevention. This allows contaminants to be accidentally introduced into the water system.

- Secure all water system access points.
- Install backflow prevention capabilities on water system elements.

Incoming water utility shares right of way with other utilities and passes under the single bridge to the site. This increases the value of the bridge as a target as well as increasing risks that maintenance on other infrastructure elements will disrupt water supply.

- Monitor maintenance on all collocated utilities.
- Establish required backup supplies of water to meet mission requirements.
- Work with supplier to remedy this SPF.
- Identify alternative sources and methods for supplying water.

Site has no knowledge/ awareness of water distribution system to site. Site can not identify or prevent suspicious activities to tamper with water supplies.

- Work with commercial provider to trace water distribution system to identify key elements.
- Implement security monitoring procedures of water system access points.

Appendix 1
Acronyms

APPENDIX A - ACRONYMS

AT	Anti-Terrorism
COOP	Continuity of Operations
DCA	Defense Critical Asset
DCIP	Defense Critical Infrastructure Program
DESC	Defense Energy Support Center
DIB	Defense Industrial Base
DoD	Department of Defense
EOD	Explosive Ordnance Disposal
HAZMAT	Hazardous Material
HVAC	Heating, Ventilation, and Air Conditioning
IA	Information Assurance
IDS	Intrusion Detection System
INFOCON	Information Condition
MHE	Materiel Handling Equipment
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NAVAIDs	Navigational Aids
SCADA	Supervisory Control and Data Acquisition
SPF	Single Point of Failure
SME	Subject-Matter Expert
UPS	Uninterruptible Power Supply

Reducing Risk...
Improving Resiliency

Office of the Assistant Secretary of Defense for
Homeland Defense and Americas' Security Affairs
OASD(HD&ASA)