UNITED STATES DEPARTMENT OF AGRICULTURE
Rural Utilities Service

Bulletin 1730B-2

SUBJECT: Guide for Electric System Emergency Restoration Plan

TO: RUS Electric Borrowers and RUS Electric Staff

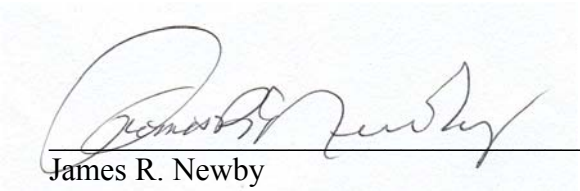
EFFECTIVE DATE: Date of Approval

OFFICE OF PRIMARY INTEREST: Electric Staff Division, Electric Program

FILING INSTRUCTIONS: This is a new bulletin and file with 7 CFR Part 1730.

AVAILABILITY: This bulletin is available on the RUS electric website at: http://www.usda.gov/rus/electric/bulletins.htm.

PURPOSE: This guide bulletin contains information to assist RUS electric borrowers in the development of a vulnerability and risk assessment (VRA) and an Emergency Restoration Plan (ERP). This guide bulletin provides references to existing resources and suggested practices with respect to security of critical electric infrastructure.



James R. Newby
Assistant Administrator, Electric Program

January 7, 2005
Date

TABLE OF CONTENTS

INDEX:

Emergency Restoration Plan (ERP)
Vulnerability and Risk Assessment (VRA)

ABBREVIATIONS

CIPC	Critical Infrastructure Protection Committee
DHS	Department of Homeland Security
DOE	U.S. Department of Energy
ERP	Emergency Restoration Plan
ES	Electric Sector
ESISAC	Electric Sector Information Sharing and Analysis Center
FBI	Federal Bureau of Investigation
FERC	Federal Energy Regulatory Commission
G&T	Generation and Transmission Cooperative
GFR	General Field Representative
HLS	Homeland Security
HSPD	Homeland Security Presidential Directive
IAIP	Information Analysis and Infrastructure Protection
IOU	Investor Owned Utility
ISAC	Information Sharing and Analysis Center
NERC	North American Electric Reliability Council
NIPC	National Infrastructure Protection Center
NRC	Nuclear Regulatory Commission
NRECA	National Rural Electric Cooperative Association
O&M	Operations and Maintenance
PDD	Presidential Decision Directive
POC	Point of Contact
PSD	Power Supply Division
REA	Rural Electrification Administration
RUS	Rural Utilities Service
SCADA	Supervisory Control and Data Acquisition Systems
VRA	Vulnerability and Risk Assessment

DEFINITIONS

Bulk transmission facilities: Are the transmission facilities connecting power supply facilities to subtransmission facilities, including both the high and low voltage sides of the transformers used to connect to the subtransmission facilities, as well as the supervisory control and data acquisition systems (SCADA).

Cyber-based systems: Electronic, radio-frequency, or computer-based information, communication, or control components or assets of a business.

Disaster: A sudden calamitous event bringing damage, loss, or destruction. *The term "disaster" lends itself to a preconceived notion of a large-scale event, usually a "natural disaster." In fact, however, each event must be addressed within the context of the impact it has on the utility and the consumer. What might constitute a nuisance to a large utility or consumer could be a "disaster" to a small utility or consumer.*

Distribution facilities: Includes all electrical lines and related facilities beginning at a consumer's meter base and continuing back to and including the distribution substation.

Emergency Management: Emergency Management is the process of preparing for, mitigating, responding to and recovering from an emergency. Emergency management is a dynamic process. Planning, though critical, is not the only component of the process. Training, conducting exercises and drills, testing equipment and coordinating activities are other important emergency management process functions.

Emergency: An emergency is any unplanned event that can involve deaths or significant injuries to employees, customers or the public, or that can shut down a business, disrupt operations, cause physical or environmental damage, or threaten a business' financial standing or public image. Numerous events can be "emergencies," including: winter storms, hurricanes, tornados, floods, earthquakes, fires, hazardous materials incidents, losses of key suppliers or customers, communications failures, chemical or radiological accidents and civil disturbances.

Generation facilities: Includes the electricity production plant and related facilities, including the building containing generation facilities, all fuel handling facilities, the step-up substation used to convert the generator voltage to transmission voltage, as well as related energy management (dispatching) systems.

Likelihood of occurrence: Defined in terms of the ease or difficulty of an action to happen in relationship to the probability of discovery or denial of action along with the time to achieve the desired results.

North America: Includes the United States, Canada and Mexico

Physical and financial loss: With respect to RUS borrowers, physical and financial loss is defined in terms of loss of life, risk to public health, impact to the ability to serve a large portion of customers for an extended period of time, impact to the reliability or operability of the energy grid, or impact to the continuity of business to the point where the repayment of RUS loan funds is jeopardized.

Private Sector: Individuals and business organizations that are not affiliated with Federal, state or local Government entities.

Subtransmission facilities: Includes the transmission facilities that connect the high voltage side of the distribution substation to the low voltage side of the bulk transmission or generating facilities, as well as related SCADA facilities.

Tabletop Exercise: A hypothetical emergency response scenario in which participants get together around a table and identify the policy, communications, resources, data, coordination, and organizational elements associated with an emergency response.

Transmission facilities: Includes all electrical lines and related facilities, including certain substations, used to connect distribution facilities to generation facilities. Transmission facilities include bulk transmission and subtransmission facilities.

FORMS

RUS Form 300, “Review Rating Summary”

1 GENERAL

This guide bulletin is to assist Rural Utilities Service (RUS) borrowers in understanding the purpose and aid in the development of a Vulnerability and Risk Assessment (VRA) and an Emergency Restoration Plan (ERP). The underlying principle of possessing an ERP is to assure the security of RUS loan funds as well the security of the electric infrastructure in rural America. The electric infrastructure covered in this guide bulletin includes the generation of energy and transmission and distribution of electric power to Rural Electrification Act (7 U.S.C. 901 et seq.) beneficiaries. This guide bulletin references and contains general methodologies, practices and planning related to procedures which support the protection of electric systems and support homeland security in the protection of the electric infrastructure. This guide bulletin outlines RUS' minimal requirements and suggested practices with respect to instituting security measures.

This guide bulletin identifies KEY provisions that should be incorporated in an ERP and provides references to assist utilities in the development of an ERP through the use of a VRA. Utilities may determine that additional provisions beyond what is discussed in this guide bulletin may be required for their system.

Making the "Case" for Emergency Management

Emergency management requires upper management support if it is to be successful. The tone is set by the chief executive by authorizing planning to take place and directing the involvement of senior management. Avoid dwelling on the negative effects of an emergency (e.g., deaths, fines, criminal prosecution,) when presenting the "case" for emergency management, and emphasize the positive aspects of preparedness, prudent utility practice and RUS requirements (when applicable). Emergency management helps companies fulfill their moral responsibility to protect employees, the community and the environment, as well as facilitates compliance with regulatory requirements of Federal, State and local agencies. Emergency management enhances a company's ability to recover from physical and financial losses, avoid regulatory fines, minimize loss of market share, minimize damage to equipment or products or business interruption and reduces exposure to civil or criminal liability in the event of an incident. Emergency management enhances a company's image and credibility with employees, customers, suppliers and the community and may reduce insurance premiums.

2 BACKGROUND

a. Legislation.

(1) Electric power systems were identified in Presidential Decision Directive 63 (PDD-63 1998) as one of the critical infrastructures of the United States. PDD-63 states, "Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the

economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private."

(2) On December 17, 2003, the President signed Homeland Security Presidential Directive -7 (HSPD-7), "Critical Infrastructure Identification, Prioritization, and Protection." This directive established a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks. HSDP-7 also directed coordination with the Private Sector in accordance with applicable laws or regulations. Federal department and sector-specific Federal agencies were directed to collaborate with appropriate private sector entities and continue to encourage the development of information sharing and analysis mechanisms. Additionally, Federal department and sector-specific Agencies were directed to collaborate with the private sector and continue to support sector-coordinating mechanisms to identify, prioritize, and coordinate the protection of critical infrastructure and key resources; and to facilitate sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices. HSDP-7 superseded PDD/NSC-63 of May 22, 1998 ("Critical Infrastructure Protection"), and any Presidential directives issued prior to this directive to the extent of any inconsistency.

b RUS Requirements.

(1) On October 12, 2004, RUS amended 7 CFR Part 1730, "Electric System Operations and Maintenance," to include the requirement that each borrower complete a vulnerability and risk assessment of its entire business (physical and cyber) and utilize the results of that assessment to create and maintain an ERP. The ERPs that are created are expected to benefit the individual electric utilities, rural America and support the national strategy for the physical and cyber security of critical infrastructures and key assets. RUS believes the security requirements set forth in 7 CFR Part 1730 are in line with Homeland Security Presidential Directives and prudent utility security practices in light of present-day concerns of threats of terrorism to the electric infrastructure of the United States.

(2) **RUS intentionally provided a degree of flexibility in the language of 7 CFR Part 1730 regarding extent of detail or specificity to provide borrowers a degree of latitude in conducting a VRA and in development of an ERP. RUS purposely did not attempt to dictate or specify a specific, unilateral, plan to all borrowers, as all electric utilities are not the same and one size does not fit all. The sheer number of variations in RUS borrowers' systems and their consumers**

make fixed templates for a standard VRA and ERP unmanageable, inefficient, fiscally imprudent and detrimental to enhancing the security of the electric sector. RUS recognizes that the borrowers themselves know their systems better than any Federal department or agency and that it is prudent that borrowers develop their own VRAs and ERPs through that knowledge.

(3) When known as the Rural Electrification Administration (REA), RUS promoted and recommended that each electric borrower have a "Disaster Plan" or "Emergency Restoration Plan" in place. The 1960 edition of REA Bulletin 60-7, "Service Reliability" stated:

> *"Every system should have an emergency plan which outlines a course of action in the event of source or substation transformer failure, excessive storm damage, ect. The plan should provide for obtaining outside help from neighboring systems and contractors when needed. The coordination of outside help with system personnel requires planning ahead of the disaster. Such details as availability of system maps, staking sheets and other records, communication facilities, housing and food for extra personnel should be considered. The plan must be tested periodically to see that it is operational."*

(4) In January of 1998, REA Bulletin 60-7 was rescinded and replaced by RUS Bulletin 1730-1, "Electric System Operation and Maintenance (O&M)." Bulletin 1730-1 further identified the need for borrowers to have an ERP. This bulletin also updated the October 1978 issuance of REA Bulletin 161-5, "Electric System Review and Evaluation." RUS Bulletin 1730-1 states that:

> *"Each borrower should have a written plan detailing how to restore its system in the event of a system wide outage resulting from a major natural disaster or other causes. This plan should include how to contact emergency agencies, borrower management and other key personnel, contractors and equipment suppliers, other utilities, and any others that might need to be reached in an emergency. It should also include recovery from loss of power to the headquarters, key offices, and/or operation center facilities. It should be readily accessible at all times under any and all circumstances."*

(5) All electric utilities including RUS borrowers utilize restoration plans in responding to service disruptions caused by natural disasters such as tornados, hurricanes, ice storms, malicious acts and major equipment failures. Not all plans have been placed in writing as the RUS regulation now requires.

(6) The September 11, 2001, attacks by terrorists and the continuing threats upon our way of life in the United States has precipitated the necessity of a next generation restoration plan to not only restore electric service after system failure but to take measures to identify possible vulnerabilities and to put in place measures to counteract these vulnerabilities and protect the electric power system.

(7) This guide bulletin details features of REA Bulletin 60-7 and RUS Bulletin 1730-1, along with new aspects, and provides guidance to borrowers for performing a VRA and developing an ERP.

(8) This bulletin does not supercede any of the requirements for nuclear power facilities as specified by the United States Nuclear Regulatory Commission (NRC) and any guidance in this document is in addition to those mandated by the NRC.

c Security Advisory System.

(1) On March 11, 2002, the President signed into law Homeland Security Presidential Directive-3 (HSPD-3). HSPD-3 established a comprehensive and effective means to disseminate information regarding the risk of terrorist acts to Federal, State, and local authorities and to the American people. The Directive decreed that the system would provide warnings in the form of a set of graduated "Threat Conditions" that would increase as the risk of the threat increases. At each Threat Condition, Federal departments and agencies would implement a corresponding set of "Protective Measures" to further reduce vulnerability or increase response capability during a period of heightened alert.

(2) The system was intended to create a common vocabulary, context, and structure for an ongoing national discussion about the nature of the threats that confront the homeland and the appropriate measures that should be taken in response. The system aspires to inform and facilitate decisions appropriate to different levels of government, the private sector, and to private citizens at home and at work. The Homeland Security Advisory System is binding on the executive branch and is suggested, on a voluntary basis, to other levels of government and the private sector.

d Threat Alert System.

(1) There are five Threat Conditions, each identified by a description and corresponding color.

Homeland Security Advisory System

Low Condition (Green).	This condition is declared when there is a low risk of terrorist attacks.
Guarded Condition (Blue).	This condition is declared when there is a general risk of terrorist attacks.
Elevated Condition (Yellow).	An Elevated Condition is declared when there is a significant risk of terrorist attacks.
High Condition (Orange).	A High Condition is declared when there is a high risk of terrorist attacks.
Severe Condition (Red).	A Severe Condition reflects a severe risk of terrorist attacks.

The higher the Threat Condition, the greater is the risk of a terrorist attack. Risk includes both the probability of an attack occurring and its potential gravity. For the Federal Government, the threat conditions are assigned by the Attorney General in consultation with the Assistant to the President for Homeland Security. Except in exigent circumstances, the Attorney General shall seek the views of the appropriate Homeland Security Principals or their subordinates, and other parties as appropriate, on the Threat Condition to be assigned. Threat Conditions may be assigned for the entire Nation, or they may be set for a particular geographic area or industrial sector. Assigned Threat Conditions are reviewed at regular intervals to determine whether adjustments are warranted.

(2) The Color-coded Threat Level System is used to communicate with public safety officials and the public at-large so that protective measures can be implemented to reduce the likelihood or impact of an attack. Raising the threat condition has economic, physical, and psychological effects on the nation. The Homeland Security Advisory System can place specific geographic regions or industry sectors on a higher alert status than other regions or industries, based on specific threat information. The national threat advisory level can be accessed through DHS at http://www.DHS.gov.

(3) The specific threat alert level system for the electric sector is posted at the Electric Sector Information Sharing and Analysis Center (ESISAC) website which can be accessed at http://www.esisac.com. The Department of Energy designated the North American Electric Reliability Council (NERC) as the Sector Coordinator for the Electricity Sector (ES). NERC, through its Critical Infrastructure Protection Committee (CIPC), has developed two guidelines related to the threat alert system: “Threat Alerts System and Physical Response Guidelines for the Electricity Sector,” and

"Threat Alerts System and Cyber Response Guidelines for the Electricity Sector." RUS encourages electric borrowers to refer to these two NERC guidelines at http://www.esisac.com/library-guidelines.htm. These guides will assist in understanding the threat alert level definitions specific to the electric sector. RUS has by federal mandate adopted the five level color coded Threat Alert System and fully supports NERC that has also adopted the federal threat alert system.

e North American Electric Reliability Council (NERC).

(1) NERC is a not-for-profit corporation whose members are comprised from the ten Regional Reliability Councils. The members of these councils come from all segments of the electric industry: investor-owned utilities, federal power agencies, rural electric cooperatives, state, municipal and provincial utilities, independent power producers, power marketers, and end-use customers. These entities account for virtually all the electricity supplied and used in the United States, Canada and a portion of Baja California Norte, Mexico. NERC was established in 1968 and since that time has grown and has operated successfully as a voluntary organization, relying on reciprocity, peer pressure and the mutual self-interest of all those involved to ensure that the bulk electric system in North America is reliable, adequate, and secure.

(2) NERC sets standards for the reliable operation and planning of the bulk electric system, monitors, assesses and enforces compliance with standards for bulk electric system reliability, provides education and training resources to promote bulk electric system reliability, coordinates critical infrastructure protection of the bulk electric system and many other functions which can be found at their website (www.nerc.com).

(3) NERC's activities are overseen by committees and working groups composed of representatives from all industry segments who provide unmatched expertise in the planning, engineering and operating aspects of electric system reliability, security, and competitive wholesale electricity markets. One subcommittee, the Critical Infrastructure Protection Committee (CIPC), oversees NERC activities promoting cyber and physical security of the industry.

f Critical Infrastructure Protection Committee (CIPC).

(1) The CIPC is one of the NERC committees that serve as the focal point for coordinating information exchange on critical infrastructure issues between the electricity industry and the federal government. The group is comprised of industry experts in the areas of cyber security, physical security, operational security, and policy from both the private and public sector. CIPC is the body that develops and coordinates NERC's security

initiatives. Through CIPC, government and industry work together to develop guidelines and best practices for utilities to draw on for information to better protect the electricity infrastructure and recover from physical and cyber attacks. This coordination ensures that the industry is able to speak with one voice and take action in a consistent and effective manner. The majority of the membership of the CIPC is comprised of electric utilities but other members include: DHS, DOE, and NRECA. RUS is an active participant in this committee. The NERC Board of Directors has approved CIPC's document entitled, "Security Guidelines for the Electricity Sector" which is comprised of fifteen individual Security Guidelines (as well as an Overview document) for the electric sector. The fifteen guidelines are:

1. Vulnerability and Risk Assessment,
2. Threat Response,
3. Emergency Plans,
4. Continuity of Business Processes,
5. Communications,
6. Physical Security,
7. Cyber Security - Risk Management,
8. Cyber Security - Access Controls,
9. Cyber Security - IT Firewalls, and
10. Cyber Security - Intrusion Detection,
11. Employment Background Screening,
12. Protecting Potentially Sensitive Information,
13. Securing Remote Access to Electronic Control and Protection Systems,
14. Threat and Incident Reporting, and
15. Physical Security – Substations

(2) RUS endorses the use of NERC security guidelines, in part or in whole, as deemed suitable, by RUS borrowers. These guidelines can be found and downloaded free of charge on the ESISAC website http://www.esisac.com/library.htm, under Security Standards and Guidelines; Threat Alert Systems.

g Electricity Sector Information Sharing and Analysis Center (ESISAC). NERC operates the Information Sharing and Analysis Center for the Electricity Sector (ESISAC). The ESISAC is utilized to share information through out the electric sector via website postings. ESISAC serves the Electricity Sector by facilitating communications between electric sector participants, the Federal government and other critical infrastructure industries and disseminates threat indications, analyses, and warnings, together with interpretations, to assist electricity sector

participants in taking protective actions. The threat alert level for the electric sector is posted and continuously updated at the ESISAC website. Utilities can obtain current ESISAC information by going to the website at http://www.esisac.com.

NOTE: Initial emergency or incident reporting of suspicious and/or malicious acts should always be to local law enforcement and local FBI.

h Department of Homeland Security, Directorate of Information Analysis and Infrastructure Protection (IAIP). The Department of Homeland Security (DHS), specifically the Directorate of Information Analysis and Infrastructure Protection (IAIP) will be the lead federal organization in coordinating the national effort to secure the nation's critical infrastructure. The DHS IAIP will have the capability to identify and assess current and future threats to the homeland; map those threats against our vulnerabilities, issue timely warnings and take preventive and protective action. The IAIP team will establish partnerships with key government, public, private and international stakeholders to create an environment that enables all partners to better protect their respective infrastructure. IAIP will also create awareness programs, develop information sharing mechanisms, and sector focused best practices and guidelines. The DHS IAIP website can be accessed at www.dhs.gov.

NOTE: Initial emergency or incident reporting of suspicious and/or malicious acts should always be to local law enforcement and local FBI.

3 VULNERABILITY AND RISK ASSESSMENT (VRA)

a A vulnerability and risk assessment is recognized as effective decision support tool for prioritizing and determining sites and functions within a business in need of security investment and development of a meaningful ERP. While it is not financially feasible to reduce risk to all potential physical and cyber targets of an electric system, vulnerability and risk assessments can help ensure that the available resources and actions taken are justified and implemented based on threat, vulnerability of a business asset to attack, and the importance of the asset. The VRA is intended to obtain the “big picture.”

(1) Title 7 CFR Part 1730 requires RUS borrowers to prepare a VRA and use it to develop an ERP. The VRA should be designed and focused to specifically identify:

- Business facilities and functions that are considered critical facilities,
- Facilities and functions with possible exposure to harm,
- Methods and methodologies to mitigate identified exposures to harm, and
- Priority of remedial attention of those identified facilities and functions, if any, to best utilize funds in the most prudent manner.

(2) Section 1730.27 requires each borrower to identify critical business asset components or elements in its system. RUS recommends that borrowers utilize the following criteria to assist in identifying critical facilities or business functions:

> "Those facilities or business functions that if damaged or destroyed would cause significant loss of life, risk to public health, negatively impact the ability to serve a large portion of its customers for an extended period of time, have a detrimental impact on the reliability or operability of the energy grid, or impact continuity of business to the point where the repayment of RUS loan funds are jeopardized."

b Vulnerability Assessment Criteria.

(1) A VRA should identify and quantify the utilities facilities, assets, or infrastructure that would have significant impact on utility operations if damaged or destroyed. The VRA should quantify the estimated criticality along with the physical and financial loss with the likelihood of occurrence. Additionally, the VRA should explore external system impacts (interdependency), if any, with loss of identified system components to other sectors or other sectors they are dependent on (i.e., transportation, telecommunications, fuel, etc.,) and any business or facility unique to the utility business that might affect homeland security concerns.

(2) **RUS does not dictate a specific method for electric borrowers to employ in developing a VRA.** Utilities need to utilize their unique knowledge of their systems to develop and execute a candid VRA specific to their system. RUS recommends that borrowers analyze the vulnerability of all their assets. Particular awareness should be given, but not limited to, facilities serving: military bases, chemical and pharmaceutical plants, hospitals and rural health clinics, fire, police, and emergency response centers. Many other critical infrastructures are dependant upon the electric sector such as: emergency medical response stations, all forms of communications facilities (telecommunications, commercial radio, television, air transportation control, etc.,) food processing and associated transportation related facilities, banks and banking facilities, and major fuel storage and pipeline facilities. **For these other critical infrastructures, it is not the responsibility of the RUS borrower to perform a VRA, develop an ERP or utilize their own funds to fortify other critical infrastructures.** RUS' desire is to emphasize that utilities need to develop (if they have not done so) bridges of communication with their customers to be able to serve their needs, particularly if they are critical infrastructures.

(3) One technique to begin the development of a VRA is for the utility to bring together personnel that have the knowledge to identify the possible events and specific physical and cyber facilities or equipment that if compromised or damaged could result in significant physical and financial loss as defined in this section. Fault tree analysis or flow charts are also good tools to utilize to identify specific events, facilities, and equipment that could result in system failure on some level of criticality. Critical assets that are identified can be ranked according to what their loss would represent.

(4) Vulnerability and threat identification is the most important step in the risk assessment process. (If vulnerabilities and threats are not accurately identified, the risks they represent cannot be reduced or eliminated). Identified vulnerabilities and associated threats are then paired with company assets. Risk-assessment identifies weaknesses in the company's critical assets that could be exploited by the threats identified and determines their nature and source. Methods used to identify vulnerabilities include evaluating data obtained through surveys and historical data from related incidents and applying formal vulnerability analysis techniques. Asset vulnerabilities can include operations and processes, policies and procedures, physical and technical security, information security, personnel security, and operations security.

(5) Mitigation or feasible actions are measures taken by the utility that either eliminate the causes or reduce the effects of one or more identified vulnerabilities. Actions can include controlling access to a facility, security cameras, personnel background investigations, new procedures, etc. The utility prudently selects actions on the basis of factors such as: whether the actions will reduce the probability of an undesired event occurring, the cost of the implementing actions, and whether there are any enforcement and audit requirements. Actions can be prioritized by considering the amount of resulting risk reduction, cost, difficulty to implement, or a combination thereof. Usually, there is a point beyond which adding countermeasures will raise costs without appreciably enhancing the protection afforded. RUS does not dictate specific actions, if any, that borrowers must employ; RUS is leaving this decision making up to the discretion of borrowers.

(6) The identification of critical transformers on a system provides a good illustration of a methodology to use for the VRA process. It is impractical to try to include all pole or pad mounted distribution transformers in a VRA or to mitigate possible threats to them. However, there will be some service transformers for which mitigation should be considered. These are transformers that supply energy to specific customers who provide services determined to be critical such as such as military facilities,

hospitals, chemical plants and pharmaceutical plants, etc. (These customers should be contacted to discuss the need for any remedial efforts and the costs, if it is decided there is a need to provide protection). Except for the special case service transformers just discussed, it is more likely that certain substation transformers, step transformers or voltage regulators and, other specific transformers critical to the utility to maintain business continuity or serve utility-identified specific customers would need to be included in a VRA. If certain substations were identified as critical and there was significant associated risk identified through the VRA, the utility would seek to implement the most cost and security effective design to mitigate the risk. For the purpose of this example the utility may decide that the most efficient and effective mitigation action would be to replace the chain link fence with a cement block, sand filled wall. This removes equipment in the substation from line of sight and reduces the possibility of someone being able to utilize a projectile (bullet) to damage equipment causing a failure and an associated outage. The utility would also need to have determined if the cost of constructing the barrier (cement block wall) was reasonable compared to the cost of repair or replacement of the equipment and the level of risk loss of that transformer will cause.

(7) RUS recognizes and recommends the use of part or all of the NERC Guide, "Vulnerability and Risk Assessment" which can be found at http://www.esisac.com/library-guidelines.htm, as well as, the "FEMA Emergency Management Guide for Business and Industry," Exhibit C to this bulletin, provides assistance in conducting a VRA on a utility system.

(8) RUS advocates that follow-up VRAs be performed when major system changes are made or if a new credible threat to the company's electric system that has not been evaluated is discovered.

c <u>Certification to RUS of Completion of VRA</u>.

(1) Section 1730.26 (b) requires RUS borrowers to send RUS written certification that they have conducted a VRA of their entire electric system and business. Borrowers with loans approved prior to July 12, 2005, are required to send a letter to RUS certifying that a VRA has been completed. This letter needs to be submitted to RUS on or prior to July 12, 2005. Distribution borrowers should send this letter to their respective Regional Divisional office. Generation and Transmission borrowers should send this letter to the RUS Power Supply Division (PSD).

(2) All loan requests submitted to RUS on or after July 12, 2005, will need to include a certification of completion of a VRA with the loan application.

(3) An example of certification language is "[ABC Electric Cooperative] certifies to RUS that on [INSERT DATE], it completed a vulnerability and risk assessment of its electric system to include both physical and cyber assets. [ABC Electric Cooperative] will retain in its records the results of the VRA." This letter is required be signed by the borrower's Manager or Chief Executive Officer.

NOTE: RUS does not want the actual VRA to be included in the loan package or sent to RUS. **Only a letter certifying that a VRA has been completed should be included in the loan application or be sent to RUS.**

d Record keeping of completed VRA. Title 7 CFR Part 1730 requires RUS borrowers to maintain in their records the results of their VRAs as well as a copy of the original letter to RUS stating that a VRA has been completed.

4 EMERGENCY RESTORATION PLAN (ERP)

a The development of an emergency restoration plan offers a utility the opportunity to prepare and plan the most efficient means in which to restore its system in the event of either a small isolated outage or a system wide outage resulting from a major natural disaster or other cause. The ERP needs to be a practical and functional tool which a utility can rely on for initial recovery efforts. It should be the foundation under which a utility, under possible adverse and confusing conditions, can begin to restore its system including both the physical (pole, wires, transformers etc.,) and cyber (telecommunications and SCADA) components and efficiently utilize its resources.

b Requirements for Compliance of Emergency Restoration Plan. Section 1730.28 requires each borrower to now have a written ERP in place and to incorporate the following in this ERP:

(1) A list of key contact emergency telephone numbers (emergency agencies, borrower management and other key personnel, contractors and equipment suppliers, other utilities, and others that might need to be reached in an emergency). RUS has provided a list of key federal emergency response numbers and contacts that need to be included in borrowers' ERPs; these telephone numbers can be found in Exhibit A of this bulletin. Borrowers should add any additional contacts that they deem suitable for their ERP.

(2) A list of key utility management and other personnel and identification of a chain of command and delegation of authority and responsibility each individual has during an emergency.

(3) Procedures for recovery from loss of power to the headquarters, key offices, and/or operation center facilities.

(4) A business continuity section describing a plan to maintain or re-establish business operations following an event which disrupts business systems. This should include computer (i.e., SCADA), telecommunications, financial (metering revenue and data) and other business systems.

(5) Any other items identified by the borrower as essential for inclusion in the ERP. RUS highly recommends that borrowers develop and include in their ERP mutual aid agreements and investigate participating in spare parts emergency supply agreements.

(6) The ERP is required to be signed by the Manager or CEO and approved by the Board of Directors.

ERP's are to be developed by the borrower through the borrower's unique knowledge of its system, prudent utility practices and the borrower's completed VRA. Most utilities presently have a storm plan that addresses the majority of the requirements of the new ERP RUS requires. In many cases, borrowers will conclude that they can simply modify their existing storm plan after completing their VRA. RUS recommends that borrowers read the NERC Security Guidelines (see paragraph 3.b.7) and to implement the components germane to their system, as well as the FEMA Emergency Management Guide for Business and Industry.

c Joint development of an Emergency Restoration Plan. Borrowers may develop a joint electric utility ERP, provided that each RUS borrower prepares an addendum to meet the requirements specified in § 1730.28 (a). The term "joint electric utilities" is intended to mean the incorporation of all **electric** utilities within an area and to include non-RUS borrowers and IOU's. Borrowers may also prepare a joint ERP utilizing their power supplier (G&T) as the lead to facilitate the creation of an ERP. RUS recognizes that there may be opportunities for borrowers to pool their resources in the development of their ERPs.

d Exercising an ERP. Title 7 CFR Part 1730 requires RUS borrowers to exercise their ERP at least annually to ensure operability and employee familiarity with the plan. A borrower may exercise its ERP in a number of ways:

(1) After a natural event (i.e., storm event) that requires the utility to utilize a significant portion of its ERP. Once recovery efforts are complete the utility can verify that the numbers and names of the Point of Contacts (POC's) listed in the ERP are correct.

(2) Participate in joint exercises with other utilities (including non-electric utilities), with other borrowers, or State or County Agencies. State or County Agencies may offset associated costs by utilization of HLS funds that may be available.

(3) Performing a tabletop exercise. A cooperative may conduct a tabletop exercise which is a hypothetical emergency response scenario in which participants get together around a table and identify the policy, communications, resources, data, coordination, and organizational elements associated with an emergency response. The tabletop exercise allows the revue of the response process and minimizes costs associated with a live exercise. This provides for a non-threatening method to exercise response, confirms understanding of procedures and provides a venue to voice concerns on responsibility.

e Certification to RUS of Completion of an ERP.

(1) Section 1730.26 (b) requires RUS borrowers to certify that they have completed and placed an ERP in place. This certification can be written in letter form. Borrowers with loans approved prior to January 12, 2006, are required to send a letter to RUS certifying that an ERP has been completed. This letter needs to be submitted to RUS on or prior to January 12, 2006. Distribution borrowers should send this letter to their respective Regional Divisional office. Generation and Transmission borrowers should send this letter to the RUS Power Supply Division.

(2) All loan requests submitted to RUS on or after January 12, 2006, will need to include a certification of completion of an ERP with the loan application.

(3) An example of certification language is "[ABC Electric Cooperative] certifies to RUS that on [INSERT DATE], it has completed a written ERP for its electric system to include both physical and cyber assets. [ABC Electric Cooperative] will retain for its records the date of establishment of the ERP. [ABC Electric Cooperative] has provided copies of its ERP to key personnel." This letter is required be signed by the borrower's Manager or Chief Executive Officer.

NOTE: RUS does not want the actual ERP to be included in the loan package or sent to RUS. **Only a letter certifying that an ERP has been completed should be included in the loan application or be sent to RUS.**

f Record keeping of completed ERP. RUS borrowers are required to maintain records that confirm that an ERP has been completed. Upon request, the records denoting that the ERP was completed, shall be made available to RUS. Borrowers need to record completion of the ERP on RUS Form 300, "Review Rating Summary." The RUS General Field Representative (GFR) who normally conducts the O&M, may request to see the ERP for the sole purpose of verifying that the ERP has been completed and is readily available for cooperative personnel. *The GFR will not be reviewing the document for content or applicability*. RUS borrowers shall also maintain, for its records, a copy of the original letter to RUS stating that an ERP has been completed.

5 REVIEW AND EVALUATION OF VULNERABILITY AND RISK ASSESSMENTS AND ERP BY RUS

a Each borrower is responsible for maintaining records of the VRA conducted and the establishment of an ERP and updates of each. Any or all of these records may be examined by RUS during its review and evaluation as identified in § 1730.24 and RUS Bulletin 1730-1, Section 2.1, Records. RUS will conduct periodic reviews of theses records to determine borrower compliance with RUS policy.

b Distribution Borrowers' Reviews.

(1) The RUS GFR is responsible, within the GFR's assigned territory, for initiating and conducting a periodic review to verify that the borrower has completed a VRA and maintains and exercises [at least annually] an ERP. The GFR will not be reviewing the VRA or ERP for content but shall validate that the borrower has an ERP that is readily available and that the borrower checked the Emergency Restoration Plan item on the RUS Form 300. The GFR is responsible for conducting this review and evaluation at least once every 3 years.

(2) If adequate information is available, the GFR will complete the review and evaluation and consult with the borrower regarding its programs and records for conducting a VRA and possessing an ERP. The GFR's signature on the RUS Form 300 signifies that the borrower has satisfied the VRA and ERP provisions to the satisfaction of RUS.

(3) If the borrower has not completed a vulnerability assessment, does not have a written ERP signed by the proper management, or has not performed and recorded, at a minimum, an annual test of operability, the GFR's review and evaluation will be deferred until the borrower has remedied the deficiencies. A borrower that is not in compliance with the VRA and ERP provisions will not be able to obtain advances of loan funds or loan approval until full compliance with 7 CFR Part 1730, in regard to the ERP, is demonstrated.

(4) Upon completion of the O&M review and evaluation, the GFR will communicate his/her findings to the borrower.

c Power Supply Borrowers.

(1) The RUS Power Supply Division (PSD) is responsible for initiating and conducting a periodic review to verify that the borrower has completed a VRA and maintains and exercises [at least annually] an ERP. PSD will not be reviewing the VRA or ERP for content but shall validate that the borrower has an ERP that is readily available and that the borrower checked the Emergency Restoration Plan item on the RUS Form 300, "Review Rating Summary." PSD will determine the frequency of this review and evaluation.

(2) If adequate information is available, the PSD representative will complete the review and evaluation and consult with the borrower regarding its programs and records for conducting a VRA and possessing an ERP. The PSD representative's signature on the RUS Form 300 signifies that the borrower has satisfied the VRA and ERP provisions to the satisfaction of RUS.

(3) If the borrower has not completed a vulnerability assessment, does not have a written ERP signed by the proper management, or has not performed and recorded, at a minimum, an annual test of operability, the PSD representative's review and evaluation will be deferred until the borrower has remedied the deficiencies. A borrower that is not in compliance with the VRA and ERP provisions will not be able to obtain advances of loan funds or loan approval until full compliance with 7 CFR Part 1730, in regard to the ERP, is demonstrated.

(4) Upon completion of the O&M review and evaluation, the PSD representative will communicate findings to the borrower.

(5) A RUS GFR may, upon request by PSD, assist in the review and evaluation, particularly with respect to transmission, sub-transmission, and substation facilities

EXHIBIT A

Federal Emergency Response Telephone and Contact Information

Criminal/Terrorist Incident To locate local office	Federal Bureau of Investigation http://www.fbi.gov/contact/fo/territory.htm
DHS/IAIP (NIPC)	http://www.dhs.gov or http://www.nipc.gov 1-202-323-3204 Email: nicc@dhs.gov Phone: 202-282-9201 Fax: 703-607-4998
U.S. National Response Team	http://www.nrt.org
Chemical Incident	National Response Center 1-888-424-8802
Biological Incident	Medical Research Institute of Infectious Diseases 1-800-872-7443
Radiation Incident	Armed Forces Radiobiology Research Institute AFRRI/MRAT 301-295-0530 1-800-SKY-PAGE PIN 801-0338 REAC/TS 8:00 AM- 4:30 PM (CST) 1-865-576-3131 AFTER 4:30 PM (CST) 1-865-576-1005
Health Incident	Health and Human Services http://www.hhs.gov Center for Disease Control http://www.cdc.gov http://www.bt.cdc.gov Public Inquires 404-639-3534 or 1-800 311-3435 Center for Disease Control and Prevention 1-404-639-3311
ESISAC	Email: esisac@nerc.com Internet: http://www.esisac.com Phone: 609-452-8060 (NERC office hours) Fax: 609-452-9550

NOTE: Any additional numbers that the utility deems needed (local hazmat, fire and police departments, etc.) should be added to this list.

EXHIBIT B

Tables of Probability and Impacts

Table I

Probability

Probability Level	Threat Level of Undesired Event	Corresponding Sector Threat Alert Level
5	Severe or Obvious	Red
4	High or Significant	Orange
3	Elevated or Considerable	Yellow
2	Guarded or Minor	Blue
1	Low or remote	Green

Table II

Impact
Levels of Criticality and Consequences

Impact Level	Criticality	Characteristics
5	Catastrophic	High mortality, acute injury, health/safety crisis, extended system loss or collapse, or severe environmental damage
4	Critical	Low mortality, severe injury, health/safety crisis, major system loss or environmental damage
3	Marginal	Minimal injury or health/safety issue, or minimal or short term system or environmental damage
2	Insignificant	No injury or health/safety event, small or short term system loss or environmental damage
1	Remote	No injury or health safety event, no system loss or environmental damage

These two general tables can be utilized to assist in categorizing the risk, threat, probability, criticality and consequences. Once the events, facilities and equipment are identified and the threat, probability and consequences have been categorized and prioritized, the utility can utilize the criteria in Tables I and II to develop matrixes to categorize the vulnerabilities and risk.

EXHIBIT C

FEMA's Sample Guide For Creating an ERP

This fundamental guide was created by FEMA and provides step-by-step advice on how to create and maintain a comprehensive emergency management program or plan. It can be used by utilities, manufacturers, corporate offices, retailers, or any organization where a sizable number of people work or gather. RUS has made slight modifications in the FEMA Guide to make it more electric sector specific.

To utilize this guide, you need not have in-depth knowledge of emergency management. What is necessary is the authority to create a plan and a commitment from the chief executive officer to make emergency management part of your corporate culture.

If you already have an Emergency Restoration Plan, as most electric utilities do (i.e., Storm Plan), use this guide as a resource to assess and update your plan.

SECTION 1 -- 4 STEPS IN THE PLANNING PROCESS

Step 1 -- Establish a Planning Team
Step 2 -- Analyze Capabilities and Hazards -- Your Vulnerability and Risk Analysis (VRA)
Step 3 -- Develop the Emergency Restoration Plan (ERP)
Step 4 -- Implement the ERP

STEP 1 -- ESTABLISH A PLANNING TEAM.

There must be an individual or group in charge of developing the ERP. The following is guidance for making the selection.

Form the Team. The size of the planning team will depend on the facility's operations, requirements and resources. Usually involving a group of people is best because:

- It encourages participation and gets more people invested in the process.
- It increases the amount of time and energy participants are able to give.
- It enhances the visibility and stature of the planning process.
- It provides for a broad perspective on the issues.

Determine who can be an active member and who can serve in an advisory capacity. In many cases, one or two people will be doing the bulk of the work. At the very least, you should obtain input from all functional areas. Remember:

- Upper management
- Line management
- Labor
- Human Resources
- Engineering and maintenance
- Safety, health and environmental affairs

- Public information officer
- Security
- Community relations
- Sales and marketing
- Legal
- Finance and purchasing

Have participants appointed in writing by upper management. Their job descriptions should be amended to reflect this important assignment.

Establish Authority. Demonstrate management's commitment and promote an atmosphere of cooperation by "authorizing" the planning group to take the steps necessary to develop a plan. The group should be led by the chief executive or the manager. Establish a clear line of authority between group members and the group leader, though not so rigid as to prevent the free flow of ideas.

Issue a Mission Statement. Have the chief executive or manager issue a mission statement to demonstrate the company's commitment to emergency management. The statement should:

- **Define the purpose of the plan** and indicate that it will involve the entire organization

- **Define the authority** and structure of the planning group

- **Establish a Schedule and Budget.** Establish a work schedule and planning deadlines. Timelines can be modified as priorities become more clearly defined. Develop an initial budget for such things as research, printing, seminars, consulting services and other expenses that may be necessary during the development process.

STEP 2 -- ANALYZE CAPABILITIES AND HAZARDS -- VRA.
This step entails gathering information about current capabilities and about possible hazards and emergencies, and then conducting a vulnerability analysis to determine the capabilities for handling emergencies.

Where Do You Stand Right Now?

Review Internal Plans and Policies
Documents to look for include:

- Storm Plan
- Restoration plan
- Mutual aid agreements
- Evacuation plan
- Fire protection plan
- Safety and health program

- Environmental policies
- Security procedures
- Insurance programs
- Finance and purchasing procedures
- Plant closing policy
- Employee manuals
- Hazardous materials plan
- Process safety assessment
- Risk management plan
- Capital improvement program

Meet with Outside Groups
Meet with government agencies, community organizations, other utilities and law enforcement. Ask about potential emergencies and about plans and available resources for responding to them. Sources of information include:

- Community emergency management office
- Mayor or Community Administrator's office
- Local Emergency Planning Committee (LEPC)
- Fire Department
- Police Department
- Emergency Medical Services organizations
- American Red Cross
- National Weather Service
- Public Works Department
- Planning Commission
- Telephone companies
- Hazardous material response teams
- Neighboring businesses

ILLUSTRATION *While researching potential emergencies, one facility discovered that a dam 50 miles away posed a threat to its community. The facility was able to plan accordingly.*

Identify Codes and Regulations
Identify applicable Federal, State and local regulations such as:

- RUS regulations
- Occupational safety and health regulations
- Environmental regulations
- Fire codes
- Seismic safety codes
- Transportation regulations
- Zoning regulations
- Corporate policies

Identify Critical Products, Services and Operations
You'll need this information to assess the impact of potential emergencies and to determine the need for backup systems. Areas to review include:

- Lifeline services such as electrical power, water, sewer, gas, telecommunications and transportation
- Products and services provided by suppliers, especially sole source vendors
- Operations, equipment and personnel vital to continued functioning
- Company products and services and the facilities and equipment needed to produce them

Identify Internal Resources and Capabilities
Resources and capabilities that could be needed in an emergency include:

- Personnel – law enforcement, hazardous materials response team, emergency medical services, security, emergency management group, evacuation team, public information officer, fire brigade.
- Equipment -- fire protection and suppression equipment, communications equipment, first aid supplies, emergency supplies, warning systems, emergency power equipment, decontamination equipment.
- Facilities -- emergency operating center, media briefing area, shelter areas, first-aid stations, sanitation facilities.
- Organizational capabilities -- training, evacuation plan, employee support system.
- Backup systems -- arrangements with other facilities to provide for:
    - Payroll
    - Communications
    - Production
    - Customer services
    - Shipping and receiving
    - Information systems support
    - Emergency power
    - Recovery support

ILLUSTRATION *One way to increase response capabilities is to identify employee skills (medical, engineering, communications, foreign language, etc.,) that might be needed in an emergency.*

Identify External Resources
There are many external resources that could be needed in an emergency. In some cases, formal agreements may be necessary to define the facility's relationship with the following:

- Local emergency management office
- Fire Department
- Hazardous materials response organization
- Emergency medical services
- Hospitals
- Local, State and Federal law enforcement
- Community service organizations
- Utilities
- Contractors
- Suppliers of emergency equipment
- Insurance carriers

Do an Insurance Review
Meet with insurance carriers to review all policies.

Conduct a Vulnerability Analysis
The next step is to assess the vulnerability of your facility -- the probability and potential impact of each emergency. Use an uncomplicated Vulnerability Analysis Chart to guide the process, which entails assigning probabilities, estimating impact and assessing resources, using a numerical system. In the example Vulnerability Analysis Chart below, the lower the score the better.

VULNERABILITY ANALYSIS CHART

(The lower the total the better)

TYPE OF EMERGENCY	Probability High 5⇔1 Low	Impacts High Impact 5 ⇔ 1 Low Impact			Resources Weak 5 ⇔ 1 Strong		TOTAL
		Human	Property	Business	Internal	External	

List Potential Emergencies

In the first column of the Vulnerability Analysis Chart, list all emergencies that could affect your facility (ies), including those identified by your local emergency management office. Consider both:

- Emergencies that could occur within your system
- Emergencies that could occur in your control area and community

Below are some other factors to consider:

- Historical -- What types of emergencies have occurred in the community, in your system or facility and at other facilities in the area?
- Severe weather
- Hazardous material spills
- Transportation accidents
- Utility outages
- Fires
- Earthquakes
- Hurricanes
- Tornadoes
- Terrorism
- Geographic -- What can happen as a result of the facility's location? Keep in mind:
    - Proximity to flood plains, seismic faults and dams
    - Proximity to companies that produce, store, use or transport hazardous materials
    - Proximity to major transportation routes and airports
    - Proximity to nuclear power plants

- Technological -- What could result from a process or system failure? Possibilities include:
    - Power failure
    - Fire, explosion, hazardous materials incident
    - Safety system failure
    - Telecommunications failure
    - Computer system failure
    - Heating/cooling system failure
    - Emergency notification system failure

- Human Error -- What emergencies can be caused by employee error? Are employees trained to work safely? Do they know what to do in an emergency? Human error is the single largest cause of workplace emergencies and can result from:
    - Poor training
    - Poor maintenance
    - Carelessness
    - Misconduct
    - Substance abuse
    - Fatigue

- Physical -- What types of emergencies could result from the design or construction of the facility? Does the physical facility enhance safety? Consider:
    - The physical construction of the facility
    - Hazardous processes or byproducts
    - Facilities for storing combustibles
    - Layout of equipment
    - Lighting
    - Evacuation routes and exits
    - Proximity of shelter areas

- Regulatory -- What emergencies or hazards are you regulated to deal with?

Analyze each potential emergency from beginning to end. Consider what could happen as a result of:

- Prohibited access to the facility
- Loss of electric power
- Communication lines down
- Ruptured gas mains
- Water damage
- Smoke damage
- Structural damage
- Air or water contamination
- Explosion
- Building collapse
- Trapped persons
- Chemical release

Estimate Probability

In the Probability column of the Vulnerability Analysis Chart, rate the likelihood of each emergency's occurrence. This is a subjective consideration. Use a simple scale of 1 to 5 with 1 as the lowest probability and 5 as the highest.

Assess the Potential Human Impact
Analyze the potential human impact of each emergency -- the possibility of death or injury. Assign a rating in the Human Impact column of the Vulnerability Analysis Chart. Use a 1 to 5 scale with 1 as the lowest impact and 5 as the highest.

Assess the Potential Property Impact
Consider the potential property for losses and damages. Again, assign a rating in the Property Impact column, 1 being the lowest impact and 5 being the highest. Consider:

- Cost to replace
- Cost to set up temporary replacement
- Cost to repair

ILLUSTRATION *The construction of a solid physical barrier at substations or switch yards such as a wall could limit the line of sight of expensive and hard to replace equipment and reduce the likelihood of damage from projectiles such as bullets.*

Assess the Potential Business Impact
Consider the potential loss of market share. Assign a rating in the Business Impact column. Again, 1 is the lowest impact and 5 is the highest. Assess the impact of:

- Business interruption
- Employees unable to report to work
- Customers unable to reach facility
- Company in violation of contractual agreements
- Imposition of fines and penalties or legal costs
- Interruption of critical supplies
- Interruption of product distribution
- Assess Internal and External Resources

Next assess your resources and ability to respond. Assign a score to your Internal Resources and External Resources. The lower the score the better. To help you do this, consider each potential emergency from beginning to end and each resource that would be needed to respond. For each emergency ask these questions:

- Do we have the needed resources and capabilities to respond?
- Will external resources be able to respond to us for this emergency as quickly as we may need them, or will they have other priority areas to serve?

If the answers are yes, move on to the next assessment. If the answers are no, identify what can be done to correct the problem. For example, you may need to:

- Develop additional emergency procedures
- Conduct additional training
- Acquire additional equipment
- Establish mutual aid agreements
- Establish agreements with specialized contractors or other utilities

ILLUSTRATION *NERC presently maintains a voluntary spare transformer database where utilities can submit requests for transformers to temporarily replace damaged transformers in cases of emergency need and until a replacement transformer can be delivered.*

Add the Columns
Total the scores for each emergency. The lower the score the better. While this is a subjective rating, the comparisons will help determine planning and resource priorities -- the subject of the pages to follow.

ILLUSTRATION *When assessing resources, remember that community emergency workers -- police, paramedics, firefighters -- will focus their response where the need is greatest. Or they may be victims themselves and be unable to respond immediately. That means response to your facility may be delayed and you should have contingencies available.*

STEP 3 -- DEVELOP THE ERP
You are now ready to develop an ERP. This section describes how.

PLAN COMPONENTS
Your plan should include the following basic components.

Executive Summary
The executive summary provides management a brief overview of: the purpose of the plan; the facility's ERP policy; authorities and responsibilities of key personnel; the types of emergencies that could occur; and where response operations will be managed.

Emergency Management Elements
This section of the plan briefly describes the facility's approach to the core elements of an ERP, which are:

- Direction and control
- Recovery and restoration
- Communications
- Life safety
- Property protection
- Community outreach

Administration and logistics.
These element, are the foundation for the emergency procedures that your facility will follow to protect personnel and equipment and resume operations.

Emergency Response Procedures
The procedures spell out how the utility will respond to emergencies. Whenever possible, develop them as a series of checklists that can be quickly accessed by senior management, department heads, response personnel and employees.

Determine what actions would be necessary to:

- Assess the situation
- Protect employees, customers, visitors, equipment, vital records and other assets, particularly during the first three days
- Get the business back up and running.

Specific procedures might be needed for any number of situations such as bomb threats or tornadoes, and for such functions as:

- Warning employees and customers
- Communicating with personnel and community responders
- Conducting an evacuation and accounting for all persons in the facility
- Managing response activities
- Activating and operating an emergency operations center
- Fighting fires
- Shutting down operations
- Protecting vital records
- Restoring operations
- Support Documents

Documents that could be needed in an emergency include:

- Emergency call lists -- lists of all persons on and off site who would be involved in responding to an emergency, their responsibilities and their 24-hour telephone numbers
- Building and site maps that indicate:
    - Utility shutoffs
    - Water hydrants
    - Water main valves
    - Water lines
    - Gas main valves
    - Gas lines
    - Electrical cutoffs
    - Electrical substations
    - Storm drains
    - Sewer lines

- Location of each building (include name of building, street name and number)
- Floor plans
- Alarm and enunciators
- Fire extinguishers
- Fire suppression systems
- Exits
- Stairways
- Designated escape routes
- Restricted areas
- Hazardous materials (including cleaning supplies and chemicals)
- High-value items
- Resource lists -- lists of major resources (equipment, supplies, services, etc.,) that could be needed in an emergency; mutual aid agreements with other companies and government agencies.

ILLUSTRATION *In an emergency, all personnel should know:*

- *What is my role?*
- *Where should I go?*

ILLUSTRATION *Some facilities are required to develop:*

- *Emergency escape procedures and routes*
- *Procedures for employees who perform or shut down critical operations before an evacuation*
- *Procedures to account for all employees, visitors and contractors after an evacuation is completed*
- *Rescue and medical duties for assigned employees*
- *Procedures for reporting emergencies*
- *Names of persons or departments to be contacted for information regarding the plan*

THE DEVELOPMENT PROCESS

The following is guidance for developing the plan:

- Identify challenges and prioritize activities
- Determine specific goals and milestones.
- Make a list of tasks to be performed, by whom and when.
- Determine how you will address the problem areas and resource shortfalls that were identified in the vulnerability analysis.

Write the Plan
Assign each member of the planning group a section to write. Determine the most appropriate format for each section. Establish an aggressive timeline with specific goals. Provide enough time for completion of work, but not so much as to allow assignments to linger. Establish a schedule for:

- First draft
- Review
- Second draft
- Tabletop exercise
- Final draft
- Printing
- Distribution

Establish a Training Schedule
Have one person or department responsible for developing a training schedule for your facility.

Coordinate with Outside Organizations
Periodically meet with or call local government agencies and community organizations. Inform appropriate government agencies that you are creating an ERP. While their official approval may not be required, they will likely have valuable insights and information to offer.

Determine State and local requirements for reporting emergencies, and incorporate them into your procedures.

Determine protocols for turning control of a response over to outside agencies. Some details that may need to be worked out are:

- Which gate or entrance will responding units use?
- Where and to whom will they report?
- How will they be identified?
- How will facility personnel communicate with outside responders?
- Who will be in charge of response activities?

Determine what kind of identification authorities will require to allow your key personnel into your facility during an emergency.

ILLUSTRATION *Your emergency planning priorities may be influenced by government regulation. To remain in compliance you may be required to address specific emergency management functions that might otherwise be a lower priority activity for that given year.*

Maintain Contact with Other Corporate Offices and Utilities
Communicate with other offices and divisions in your company or others utilities to learn:

- Their emergency notification requirements
- The conditions where mutual assistance would be necessary
- How offices will support each other in an emergency
- Names, telephone numbers and pager numbers of key personnel

Incorporate this information into your procedures.

Review, Conduct Training and Revise
Distribute the first draft to group members for review. Revise as needed.

For a second review, conduct a tabletop exercise with management and personnel who have a key emergency management responsibility. In a conference room setting, describe an emergency scenario and have participants discuss their responsibilities and how they would react to the situation. Based on this discussion, identify areas of confusion and overlap, and modify the plan accordingly.

Seek Final Approval
Arrange a briefing for the chief executive officer and senior management and obtain written approval.

Distribute the Plan
Place the final plan in three-ring binders and number all copies and pages. Each individual who receives a copy should be required to sign for it and be responsible for posting subsequent changes.

Determine which sections of the plan would be appropriate to show to government agencies (some sections may refer to corporate secrets or include private listings of names, telephone numbers or radio frequencies). Distribute the final plan to:

- Chief executive and senior managers
- Key members of the company's emergency response organization
- Company headquarters
- Community emergency response agencies (appropriate sections)

Have key personnel keep a copy of the plan in their homes. Inform employees about the plan and training schedule.

ILLUSTRATION *Consolidate emergency plans for better coordination. Stand-alone plans, such as a Storm Plan, Spill Prevention Control and Countermeasures (SPCC) plan, fire protection plan or safety and health plan, should be incorporated into one comprehensive plan.*

STEP 4 -- IMPLEMENT THE PLAN.
Implementation means more than simply exercising the plan during an emergency. It means acting on recommendations made during the vulnerability analysis, integrating the plan into company operations, training employees and evaluating the plan.

INTEGRATE THE PLAN INTO COMPANY OPERATIONS
Emergency planning must become part of the corporate culture.
Look for opportunities to build awareness; to educate and train personnel; to test procedures; to involve all levels of management, all departments and the community in the planning process; and to make emergency management part of what personnel do on a day-to-day basis.

Test how completely the plan has been integrated by asking:

- How well does senior management support the responsibilities outlined in the plan?
- Have emergency planning concepts been fully incorporated into the facility's accounting, personnel and financial procedures?
- How can the facility's processes for evaluating employees and defining job classifications better address emergency management responsibilities?
- Are there opportunities for distributing emergency preparedness information through corporate newsletters, employee manuals or employee mailings?
- What kinds of safety posters or other visible reminders would be helpful?
- Do personnel know what they should do in an emergency?
- How can all levels of the organization be involved in evaluating and updating the plan?

CONDUCT TRAINING, DRILLS AND EXERCISES
Everyone who works at or visits the facility requires some form of training. This could include periodic employee discussion sessions to review procedures, technical training in equipment use for emergency responders, evacuation drills and full-scale exercises. Below are basic considerations for developing a training plan.

- **Planning Considerations**
  Assign responsibility for developing a training plan. Consider the training and information needs for employees, contractors, visitors, managers and those with an emergency response role identified in the plan.

  Determine for a 12 month period:

  - Who will be trained?
  - Who will do the training?
  - What training activities will be used?
  - When and where each session will take place?
  - How the session will be evaluated and documented?

Consider how to involve community responders in training activities. Conduct reviews after each training activity. Involve both personnel and community responders in the evaluation process.

- **Training Activities**
  Training can take many forms:

  - Orientation and Education Sessions -- These are regularly scheduled discussion sessions to provide information, answer questions and identify needs and concerns.
  - Tabletop Exercise -- Members of the emergency management group meet in a conference room setting to discuss their responsibilities and how they would react to emergency scenarios. This is a cost-effective and efficient way to identify areas of overlap and confusion before conducting more demanding training activities.
  - Walk-through Drill -- The emergency management group and response teams actually perform their emergency response functions. This activity generally involves more people and is more thorough than a tabletop exercise.
  - Functional Drills -- These drills test specific functions such as medical response, emergency notifications, warning and communications procedures and equipment, though not necessarily at the same time. Personnel are asked to evaluate the systems and identify problem areas.
  - Evacuation Drill -- Personnel walk the evacuation route to a designated area where procedures for accounting for all personnel are tested. Participants are asked to make notes as they go along of what might become a hazard during an emergency, e.g., stairways cluttered with debris, smoke in the hallways. Plans are modified accordingly.
  - Full-scale Exercise -- A real-life emergency situation is simulated as closely as possible. This exercise involves company emergency response personnel, employees, management and community response organizations.

- **Employee Training**
  General training for all employees should address:
  - Individual roles and responsibilities
  - Information about threats, hazards and protective actions
  - Notification, warning and communications procedures
  - Means for locating family members in an emergency
  - Emergency response procedures
  - Evacuation, shelter and accountability procedures
  - Location and use of common emergency equipment
  - Emergency shutdown procedures

  The scenarios developed during the vulnerability analysis can serve as the basis for training events.

ILLUSTRATION *OSHA training requirements are a minimum standard for many facilities that have a fire brigade, hazardous materials team, rescue team or emergency medical response team.*

- **Evaluate and Modify the Plan**
  Conduct a formal audit of the entire plan at least once a year. Among the issues to consider are:
  - How can you involve all levels of management in evaluating and updating the plan?
  - Are the problem areas and resource shortfalls identified in the vulnerability analysis being sufficiently addressed?
  - Does the plan reflect lessons learned from drills and actual events?
  - Do members of the emergency management group and emergency response team understand their respective responsibilities? Have new members been trained?
  - Does the plan reflect changes in the physical layout of the facility? Does it reflect new facility processes?
  - Are photographs and other records of facility assets up to date?
  - Is the facility attaining its training objectives?
  - Have the hazards in the facility changed?
  - Are the names, titles and telephone numbers in the plan current?
  - Are steps being taken to incorporate emergency management into other facility processes?
  - Have community agencies and organizations been briefed on the plan? Are they involved in evaluating the plan?

  In addition to a yearly audit, evaluate and modify the plan at these times:
  - After each training drill or exercise
  - After each emergency
  - When personnel or their responsibilities change
  - When the layout or design of the facility changes
  - When policies or procedures change

  Remember to brief personnel on changes to the plan.