RUS 2004 ELECTRIC ENGINEERING SEMINAR

FEBRUARY 10-11, 2004

NEW ORLEANS, LA

Critical Infrastructure Protection
RUS Security Requirements

John Pavek

Chief, Distribution Branch

RUS Homeland Security Representative.

BIOGRAPHICAL SKETCH

JOHN PAVEK

John Pavek is the Distribution Branch Chief of the Electric Staff Division. John is also the RUS Homeland Security Representative, a member of the Rural Development Homeland Security Task Force, the North American Electric Reliability Councils Critical Infrastructure Protection Advisory Group and has represented the USDA on a number of the Homeland Security Councils Policy Coordination Committees. John has a Master of Arts degree in National Security and Strategic Studies and a diploma from the College of Command and Staff from the United States Naval War College in Newport, Rhode Island. John obtained his undergraduate degree from the State University of New York Maritime College in Marine/Mechanical Engineering with a minor in Nuclear Engineering. John was an Officer in the United States Navy Reserve from 1985 till 1994. John has worked in the electric utility industry since 1988 as a lineman; line supervisor and a system operator for Investor owned utilities in New York State and joined RUS in 1998. Prior to working in the electric utility industry, John sailed as First and Chief Engineer on various Tugboats and Tankers out of New York.

Critical Infrastructure Protection –RUS Security Requirements

The September 11 attacks highlighted terrorists are capable of causing enormous damage by attacking our critical infrastructure. The August 14, 2003, Northeast Power Outage further identified the electric grid as a target and some of its weaknesses.

Critical Infrastructures Defined

Physical and virtual systems and assets that are so essential to the minimum operations of government and the economy that the incapacity of such systems and assets would have a debilitating impact on national security; economic security; public health or safety; or any combination of these.

Critical Infrastructure

Critical infrastructures have been identified as energy sources to include: electrical, nuclear, gas, oil, and dams, information and telecommunications networks, water, food, agriculture, health and emergency services, transportation to include: air, road, rail, ports and waterways, banking and finance systems, and postal systems.

Basic Principles of Protecting Critical Infrastructure

Some of the basic principle that assists in the protection of America's critical infrastructure include: surveillance, two-way communications and the understanding that it is a shared responsibility of the Federal Government, State Government, Local Government and the private sector.

Electric utilities need to develop and maintain Plans and Procedures, Orders of Succession, Delegations of Authority, Alternate Facilities, Interoperable Communications, Vital files, Records & Databases, Exercises, training & testing and define Essential Functions.

Plans and Procedures

A utility should develop a plan that: delineates essential functions and activities; outlines a decision process for determining appropriate actions and implementing plans & procedures; and establishes a roster of emergency personnel with authority to perform essential functions. The plan should also include procedures for employee advisories, alerts and emergency restoration plan activation.

Orders of Succession

Orders of succession need to be established for the organization head and for other key headquarters leadership positions. These orders should identify limitations of authority and establish rules and procedures addressing: condition of succession, method notification and time, geographical, and organization limitations.

Delegation of Authority

- Identify programs & administrative authorities needed
- Identify which authorities can/should be delegated
- Identify circumstances in which specific authorities becomes effective

Alternate Facilities

- Capable of supporting operations in threat free environment
- Interoperable communications
- Reliable logistical support services & infrastructure systems
- Appropriate physical security & access controls
- Health, safety & emotional well being of personnel

Vital Files, Records & Data Bases

A utility must protect and back up vital files, records and databases (VFRDB) to ensure the ability to continue business operations with the loss of access to its headquarters. Some examples of VFRDB are: business, legal & financial records, personnel, payroll, insurance, contracts, customers, emergency operating records, plans & directives, orders of succession, and delegation of authority and staffing assignments

Exercises, Training & Testing

In order to properly assess the viability of an emergency restoration plan, particularly under emergency or stressful conditions, a utility must exercise and test the plan. Such testing will create a familiarity with the plan and its procedures. A utility should incorporate exercises for individual & team (G&T with Distribution members) personnel. Internal exercising of emergency plans and procedures, testing of alert and notification systems, joint utility exercising of emergency plans and procedures (Mutual Aid) and refresher orientation should be performed annually.

REA/RUS Previous Requirements

- REA BULLETIN 60-7 (1960)
- RUS BULLETIN 1730-1 (1998)

RUS Security Requirements

A borrower will need to perform a vulnerability and risk assessment of its own system for both the physical and cyber elements of all plant. The assessment should consider who the system serves, identify specific critical components unique to the system and determine if components are crucial to the utility and possibly national security.

The utility has the option to perform a self assessment or hire a contractor which can be a G&T (energy provider). Borrowers can obtain vulnerability and risk assessment information from DHS - Protective Security Division, DOE, NRECA (which maintains a contractors list) or pick a contractor on their own. The vulnerability and risk assessment will be self-certified.

Emergency Restoration Plan

RUS is not planning on dictating a specific, unilateral Emergency Restoration Plan (ERP) as all utilities are not the same and one size does not fit all. RUS does expect borrowers' ERPs to incorporate consideration of unnatural disasters to include terrorism both domestic & foreign.

RUS expects borrowers' ERP's to exist in written form, be certified and signed by top management (CEO, Manager, etc.,) and that copies must be readily available to key personnel. RUS also expects the ERP's to be exercised annually, at a minimum, to ensure operability and employee competency while also serving to identify and correct deficiencies that manifest themselves during testing. Borrowers will indicate the existence and their annual testing of the ERP by appropriately recording information on Part II, "Operations and Maintenance" of RUS Form 300, "Review Rating Summary.". A borrower's ERP must also include a business continuity section, identify Key Utility Management Personnel, incorporate a chain of command and delegation authority, include a spare parts emergency supply agreement on critical items with Equipment Suppliers or other utilities, and serve to develop and maintain Mutual Aid Agreements. The ERP must have key emergency contact telephone (land and cell) numbers such as: Local, State & Federal Law Enforcement (FBI), Federal Emergency Management Agency (FEMA), chemical, biological, radiological, and health incident response teams.

Federal Guidance

- The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets: www.whitehouse.gov/pcipb/physical.html
- National Strategy for Homeland Security: www.whitehouse.gov/homeland/book
- The National Strategy to Secure Cyberspace: www.whitehouse.gov/pcipb

Private Sector Guidance

- North American Electric Reliability Council's Critical Infrastructure Protection Advisory Group
- Guidelines for Physical and Cyber Security: www.nerc.com

Presidential Decision Directives

- PDD – 63 May 22, 1998 Critical Infrastructure Protection
- Executive Order 13228 October 8, 2001 Establishing Office of Homeland Security

- Executive Order 13231 October 16, 2001 Critical Infrastructure Protection in the Information Age
- HSPD-1 October 29, 2001 Organization & Operation of the Homeland Security Council
- HSPD-5 February 28, 2003 Management of Domestic Incidents
- HSPD-7 December 17 2003 Critical Infrastructure Identification, Prioritization, and Protection

RUS 2004 Electric Engineering Seminar

John B. Pavek
Branch Chief
Electric Staff Division
RUS Homeland Security

February 10, 2004

Critical Infrastructure Protection

- September 11 attacks highlighted terrorists are capable of causing enormous damage by attacking our critical infrastructure
- August 14, 2003, Northeast Power Outage further identified the electric grid as a target

August 14, 2003 Blackout

- 21 power plants shut down in 3 minutes (10 nuclear)
- Impacted area covering 50 million people
- 9,300 sq. miles without power
- 62,000 MW of power lost
- Worst blackout in US history
- **Cascading effects across all critical infrastructures**

Courtesy of DOE OEA

3

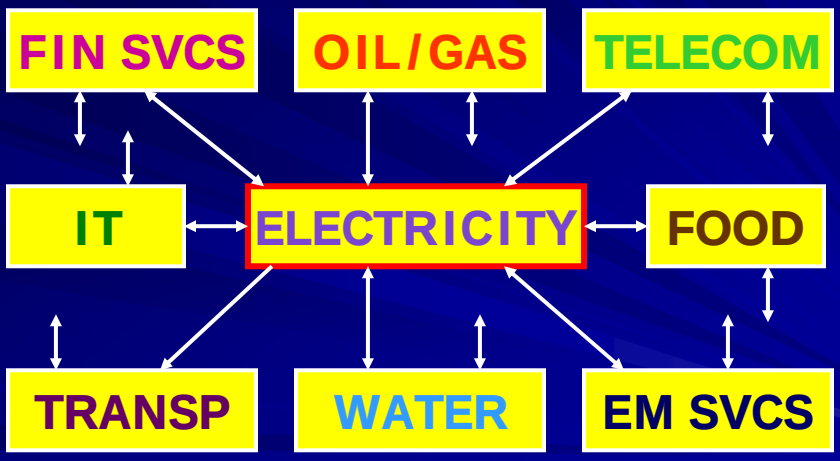
Critical Infrastructures Defined

- **USA Patriot ACT of 2001**
  - systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on:
  - Security
  - National economic security
  - National public health or safety
  - Any combination of those matters

Rural Utilities Service
Homeland Security

4

Interdependency on Electricity



Critical Infrastructure

- Energy sources
  - Electrical
  - Nuclear
  - Gas
  - Oil
  - Dams
- Information and telecommunications networks
- Water
- Food

Critical Infrastructure

- Agriculture
- Health and Emergency Services
- Transportation
  - Air
  - Road
  - Rail
  - Ports
  - Waterways
- Banking and Finance Systems
- Postal Systems

Protecting America's Critical Infrastructure

- Surveillance
- Communications
- Shared responsibility
  - **Federal Government**
  - **State Government**
  - **Local Government**
- Active partnership
  - **Private sector - 85 % Critical Infrastructure**

VIABLE CAPABILITY

- Plans and Procedures
- Essential Functions
- Orders of Succession
- Delegations of Authority
- Alternate Facilities
- Interoperable Communications
- Vital files, Records & Databases
- Exercises, training & testing

Plans and Procedures

- PREPARE CLEAR, UNCOMPLICATED PLANS AND CLEAR, CONCISE ORDERS TO ENSURE THOROUGH UNDERSTANDING
  - Broad strategies and guidance, rather than detailed instructions, encourage flexibility
  - Direct, simple plans reduce misunderstanding and confusion
  - Simple plans executed promptly are preferred over complex plans executed later

Plans and Procedures

- Develop a plan that:
  - Delineates essential functions and activities
  - Outlines a decision process for determining appropriate actions, implementing plans & procedures
  - Establishes a roster of emergency personnel with authority to perform essential functions
  - Includes procedures for employee advisories, alerts and emergency restoration plan activation

Plans and Procedures

“Make your plans to fit the circumstances.“

"A good plan executed today is better than a perfect plan executed at some indefinite point in the future."

General George S. Patton, Jr.

Orders of Succession

- Establish for Organization Head
- Establish for other key headquarters leadership position
- Identify Limitations of Authority
- Establish rules and procedures addressing:
  - Condition of succession
  - Method Notification
  - Time, geographical, organization limitations

Delegation of Authority

- Identify programs & administrative authorities needed
- Identify which authorities can/should be delegated
- Identify circumstances in which becomes effective

Alternate Facilities

- Capable of supporting operations in threat free environment
- Interoperable communications
- Reliable logistical support services & infrastructure systems
- Appropriate physical security & access controls
- Health, safety & emotional well being of personnel

Vital Files, Records & Data Bases

- Business, Legal & Financial Records
  - Personnel
  - Payroll
  - Insurance
  - Contracts
  - Customers
- Emergency Operating Records
  - Plans & directives
  - Orders of succession
  - Delegation of authority
  - Staffing assignments

Exercises, Training & Tests

- Individual & team (G&T with Dist. Members)
- Internal exercising of emergency plans and procedures
- Testing of alert and notification system
- Refresher orientation
- Joint utility exercising of emergency plans and procedures (Mutual Aid)

REA/RUS PREVIOUS REQUIREMENTS

- *REA BULLETIN 60-7 (1960)*

"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, etc. 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."

REA/RUS
PREVIOUS REQUIREMENTS

- *RUS BULLETIN 1730-1 (1998)*

"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."

Homeland Security

- RUS will be amending 7 CFR Part 1730 to establish policy to include Homeland Security measures. It will require that borrowers of RUS funds perform a vulnerability and risk assessment (physical and cyber) on their systems and establish and exercise an emergency restoration plan. Publication of the proposed rule is expected early 2004.

NO ERP = NO $$$

RUS Emergency Restoration Plan Time Line

Initiating Events
Determination whether Rule is Needed
Preparation of Proposed Rule
Internal Review of Proposed Rule
Publication of Proposed Rule
  30 day Comment Period
  Review & Evaluate Comments
Preparation of Final Rule
Publication of Final Rule
Electric System Emergency Restoration Bulletin

RUS Security Requirements

- **VULNERABILITY / RISK ASSESSMENT**
  CO-OP's will need to perform a vulnerability and risk assessment of its own system
- Physical and Cyber
  - Consider who the system serves
  - Identify specific critical components unique to the system
  - Determine if components are crucial to the utility and possibly national security

RUS Security Requirements

vulnerability assessment cont.

Who Performs Assessment ??
- Self Assessment
- G&T
- Contractor

Where to get vulnerability assessment information ??
- DHS
  - Protective Security Division
- DOE
  - Office of Energy Assurance
- NRECA
  - Contractor list
- NERC

✓ **SELF CERTIFIED**

RUS Security Requirements

EMERGENCY RESTORATION PLAN

- Incorporate unnatural disasters to include terrorism (domestic & foreign)
- RUS not planning on dictating a specific, unilateral Emergency Restoration Plan (ERP)
- All utilities are not the same and one size does not fit all

RUS Security Requirements

EMERGENCY RESTORATION PLAN

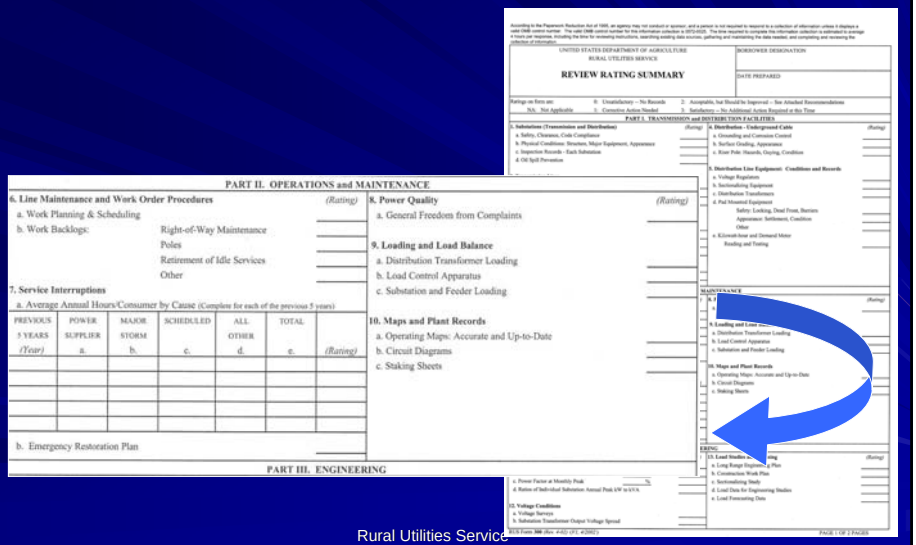
- Exist in written form, be certified and signed by the borrower's CEO and Manager and approved by the Board of Directors
- Copies must be readily available to key personnel
- Include a business continuity section

RUS Security Requirements

Emergency Restoration Plan

- It must be exercised annually, at a minimum, to ensure operability and employee competency
- Serve to identify and correct deficiencies that manifest themselves during testing
- Recorded on RUS Form 300, Part II. Operations and Maintenance verifying compliance

RUS Form 300


UNITED STATES DEPARTMENT OF AGRICULTURE
RURAL UTILITIES SERVICE

REVIEW RATING SUMMARY

BORROWER DESIGNATION

DATE PREPARED

PART I. TRANSMISSION and DISTRIBUTION FACILITIES

PART II. OPERATIONS and MAINTENANCE

6. Line Maintenance and Work Order Procedures (Rating)
a. Work Planning & Scheduling
b. Work Backlogs:
Right-of-Way Maintenance
Poles
Retirement of Idle Services
Other

7. Service Interruptions
a. Average Annual Hours/Consumer by Cause (Complete for each of the previous 5 years)

PREVIOUS 5 YEARS (Year)	POWER SUPPLIER a.	MAJOR STORM b.	SCHEDULED c.	ALL OTHER d.	TOTAL e.	(Rating)

b. Emergency Restoration Plan

8. Power Quality (Rating)
a. General Freedom from Complaints

9. Loading and Load Balance
a. Distribution Transformer Loading
b. Load Control Apparatus
c. Substation and Feeder Loading

10. Maps and Plant Records
a. Operating Maps: Accurate and Up-to-Date
b. Circuit Diagrams
c. Staking Sheets

PART III. ENGINEERING

RUS Security Requirements

EMERGENCY RESTORATION PLAN

- Identify Key Utility Management Personnel and incorporate a chain of command and delegation of authority
- Have a spare parts emergency supply agreement on critical items with Equipment Suppliers or other utilities

RUS Security Requirements

EMERGENCY RESTORATION PLAN

- Develop and maintain a Mutual Aid Agreements and flowcharts
- It must have key emergency contact numbers
  - Local, State & Federal Law Enforcement (FBI)
  - Federal Emergency Management Agency (FEMA)
  - Chemical, Biological Radiological & Health Incident Response Teams

EMERGENCY RESPONSE TELEPHONE NUMBERS

- **Chemical Incident** — **National Response Center**
  www.nrc.uscg.mil/ **1-888-424-8802**
  202-267-2675
- **Biological Incident** — **Medical Research Institute of Infectious Diseases**
  www.usamrid.army.mil/ **1-888-872-7443**
- **Radiation Incident** — **Armed Forces Radiobiology Research Institute**
  www.affri.usuhs.mil/
  AFRRI/MRAT **(301) 295-0530**
  1-800-SKY-PAGE **Pin 801-0338**

  Radiation Emergency Assistance Center
  www.orau.gov/reacts/
  8:00 a.m.-4:30 p.m. (CST) **(865) 576-3131**
  After 4:30 p.m. (CST) **(865) 576-1005**

EMERGENCY RESPONSE TELEPHONE NUMBERS

- **Health Incident** — **Health and Human Services** — **www.hhs.gov** / **www.dhhs.gov**

  Center for Disease Control — **www.cdc.gov** / **www.bt.cdc.gov**

  Public Inquiries — **(404) 639-3534** / **(800) 311-3435**

  Centers for Disease Control and Prevention (24/7) — **(404) 639-3311**

  Hot Line 888-246-2675

- **Criminal or Terrorist Incident**

  Federal Bureau of Investigation

  www.fbi.gov/contact/fo/territory.htm

  National Infrastructure Protection Center

  www.nipc.gov **(202) 323-3205**

  Toll free: 888-585-9078

Construction Changes for Security

What specific physical security changes is RUS looking at ????

"Never tell people how to do things. Tell them what to do and they will surprise you with their ingenuity."

General George S. Patton, Jr.

Federal Guidance

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

www.whitehouse.gov/pcipb/physical.html

National Strategy for **Homeland Security**

www.whitehouse.gov/homeland/book

The National Strategy to **Secure Cyberspace**

www.whitehouse.gov/pcipb

Private Sector Guidance

North American Electric Reliability Council's Critical Infrastructure Protection Advisory Group Guidelines for Physical and Cyber Security

www.nerc.com

Presidential Decision Directives

- PDD – 63
  - May 22, 1998 — Critical Infrastructure Protection
- Executive Order 13228
  - October 8, 2001 — Establishing Office of Homeland Security
- Executive Order 13231
  - October 16, 2001 — Critical Infrastructure Protection in the Information Age
- HSPD -1
  - October 29, 2001 — Organization & Operation of the Homeland Security Council
- HSPD -5
  - February 28, 2003 — Management of Domestic Incidents
- HSPD – 7
  - December 17, 2003 — Critical Infrastructure Identification, Prioritization, and Protection

FINALTHOUGHTS

"After we have thought out everything carefully in advance and have sought and found without prejudice the most plausible plan, we must not be ready to abandon it at the slightest provocation. Should this certainty be lacking, we must tell ourselves that nothing is accomplished in warfare without daring; that the nature of war certainly does not let us see at all times where we are going; that what is probable will always be probable though at the moment it may not seem so; and finally, that we cannot be readily ruined by a single error, if we have made reasonable preparations."

Karl von Clausewitz