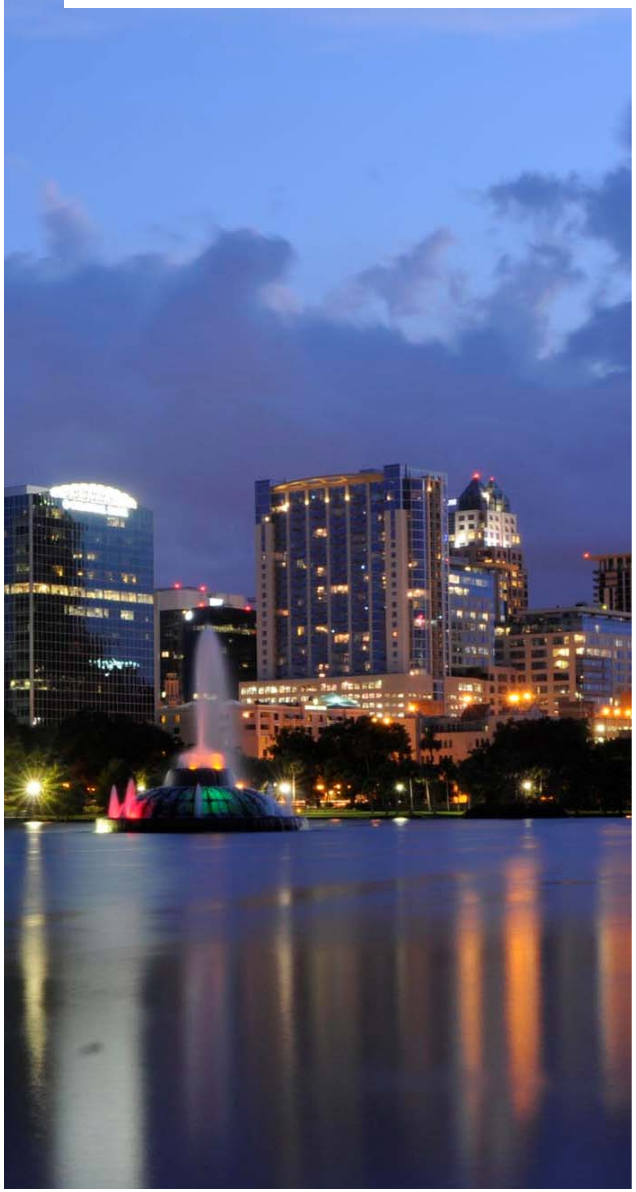


SIEMENS

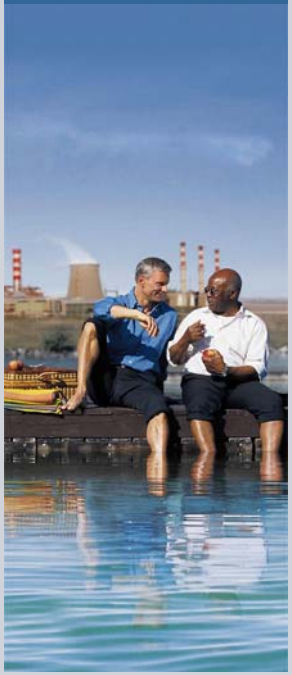
Supporting our customers with NERC CIP compliance

James McQuiggan, CISSP

SIEMENS

Siemens Energy Sector

Energy products and solutions - in 6 Divisions

Oil & Gas	Fossil Power Generation	Renewable Energy	Service Rotating Equipment	Power Trans-mission	Power Distribution
					

SIEMENS

Enterprise Wide Power Generation Management

Waste-fired Cogeneration Plants

Coal-fired Power Plants

Wind Power Plants

Combined Cycle Plants

Nuclear Power Plants

Desalination Plants

Industrial Power Plants

Coal Gasification Plants

Biomass Power Plants

District Heat Power Plants

Mapping the CIP Standards to Siemens competencies

SIEMENS

CIP Version 1 Current Standards

- CIP 001 – Sabotage Reporting
- CIP 002 – CCA Identification
- CIP 003 – Security Management
- CIP 004 – Personnel, Training
- CIP 005 – Electronic Security
- CIP 006 – Physical Security
- CIP 007 – Systems Security
- CIP 008 – Incident Reporting & Response
- CIP 009 – Recovery Plans

- Siemens CERT – Cyber asset security and expertise (003, 005,007)
- Global Data Pool – international personnel tracking and notification (004)
- Learn@ Siemens – NERC CIP CBT (004)
- Relationship with Verifications Inc (004)
- Information Security Program (004)
- Physical Security Expertise through Siemens Industry – Building Technologies Division (006)
- Expert I&C controls / Support (005, 007, 009)
- Member NERC Standards Committee (all)
- Security Consulting Services (all)
- CISSP, CPP Coordination (all)

Siemens Capabilities to the NERC CIP Standards

SIEMENS

Siemens NERC CIP Policies

- NERC CIP Compliance Database

- Customer Notifications
  - 12 hours of termination
  - 7 days for other changes
- Track employees training and background checks

- Siemens Critical Cyber Asset Training Program

- Specific for CCA's or BES cyber systems
- Remote Access policies and procedures from Siemens (cRSP)

SIEMENS

Siemens NERC CIP Policies

- Personal Risk Assessments
- 3rd party background check company

- Secure web-based screening
- ISO 9001:2000 certified
- Local and state for all 50 states

- Security Awareness Program

- Bi-annual manager and employee online training
- New-hire orientation program
- Information security advisor program
- Company Newsletters
- Internal control system – audits on information security

SIEMENS

NERC CIP Cyber Security Standards

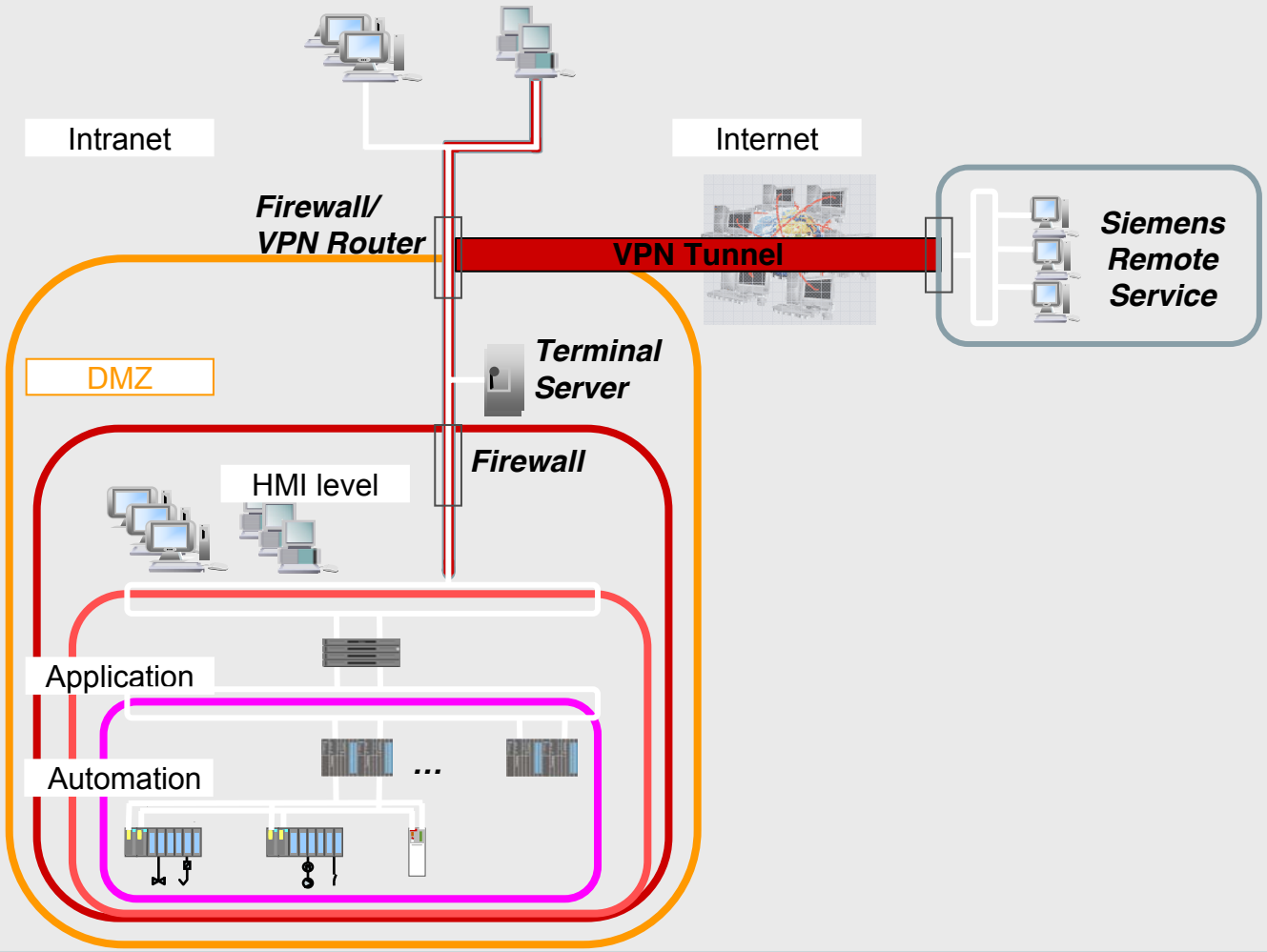
CIP002-009 - Eight Standards / 41 Requirements

CIP-002	CIP-003	CIP-004	CIP-005	CIP-006	CIP-007	CIP-008	CIP-009
CRITICAL CYBER ASSETS	**SECURITY MANAGEMENT CONTROLS**	**PERSONNEL AND TRAINING**	**ELECTRONIC SECURITY**	**PHYSICAL SECURITY**	**SYSTEMS SECURITY MANAGEMENT**	**INCIDENT REPORTING & RESPONSE PLANNING**	**RECOVERY PLANS FOR CCA**
1. CRITICAL ASSETS 2. CRITICAL CYBER ASSETS 3. ANNUAL REVIEW 4. ANNUAL APPROVAL	1. CYBER SECURITY POLICY 2. LEADERSHIP 3. EXCEPTIONS 4. INFORMATION PROTECTION 5. ACCESS CONTROL 6. CHANGE CONTROL	1. AWARENESS 2. TRAINING 3. PERSONNEL RISK ASSESSMENT 4. ACCESS	1. ELECTRONIC SECURITY PERIMETER 2. ELECTRONIC ACCESS CONTROLS 3. MONITORING ELECTRONIC ACCESS 4. CYBER VULNER-ABILITY ASSESSMENT 5. DOCUMEN-TATION	1. PLAN 2. PHYSICAL ACCESS CONTROLS 3. MONITORING PHYSICAL ACCESS 4. LOGGING PHYSICAL ACCESS 5. ACCESS LOG RETENTION 6. MAINTE-NANCE & TESTING Siemens Building Technology (SBT)	1. TEST PROCEDURES 2. PORTS & SERVICES 3. SECURITY PATCH MANAGEMENT 4. MALICIOUS SOFTWARE PREVENTION 5. ACCOUNT MANAGEMENT 6. SECURITY STATUS MONITORING 7. DISPOSAL OR REDEPLOY-MENT 8. CYBER VULNERABILITY ASSESSMENT 9. DOCUMEN-TATION	1. CYBER SECURITY INCIDENT RESPONSE PLAN 2. DOCUMEN-TATION	1. RECOVERY PLANS 2. EXERCISES 3. CHANGE CONTROL 4. BACKUP & RESTORE 5. TESTING BACKUP MEDIA

BLACK – Customer Responsibility
RED – T3000 Feature
BLUE – Siemens Service

SIEMENS

SPPA-T3000 Control System Security Features



- SPPA-T3000 ESP and security zone architecture (Defense in Depth)
- Secure remote access
- Monitoring
- Malware protection software
- Account management
- Security patch management

SIEMENS

Getting Security "Baked-in"

- Work with your vendors to have the security baked in the products
  - They want to make "you" reliable AND secure
  - Flexibility, documentation and agreements (contracts)
- DHS Procurement Language
  - Helpful to assisting you with getting secure & reliable product
  - Discuss the OEM / Vendor security policies
- Develop a policy for vendors, 3rd party companies
  - Personal Risk Assessments
  - Training of their products

SIEMENS

Questions ?