GovEnergy
www.govenergy.gov

· August 15-18, 2010 · Dallas, Texas ·
· Dallas Convention Center ·

DoD Information Assurance for Industrial Control Systems

Real Property in DoD Enterprise

- DoD, like virtually all customer-centric businesses, is an enterprise
  - More than 535,000 real property assets with plant replacement value of $700B+
    - Aging from new to Revolutionary War-era
    - Each asset has or is comprised of at least one industrial control or building automation system
  - More than 6,000 sites in US and more than 30 countries
  - Expenditures of $54B+/year for Installations & Environment programs
  - Almost 300 different installation management systems

Industrial Control and Building Automation Systems in DoD

- Energy Management Systems/Direct Digital Control (EMS/DDC): used to monitor and control facilities systems (e.g., HVAC, lighting)

- Supervisory Control And Data Acquisition (SCADA): real-time supervisory control systems for utilities production and distribution

- Advanced Meter Infrastructure (AMI): measures utility usage, as well as power quality in electrical distribution systems

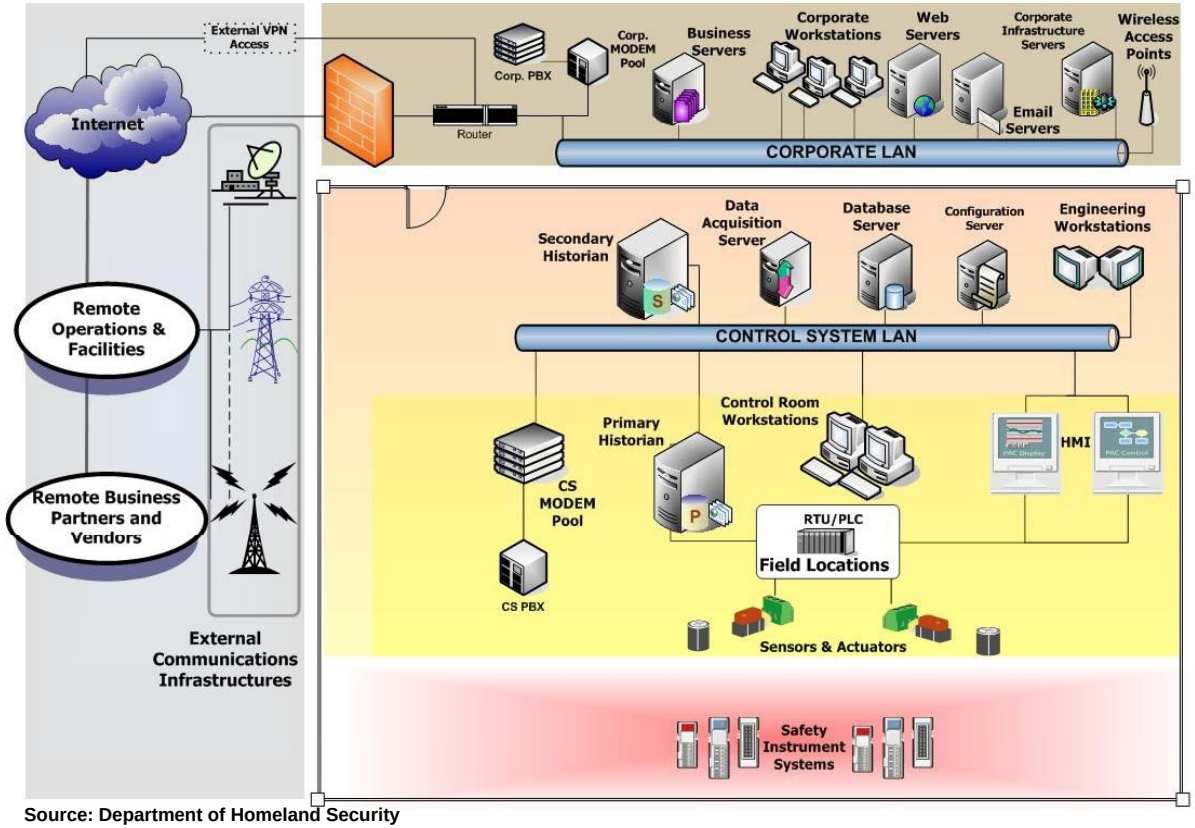
- Other systems include lighting, video monitoring, fire alarm, fire suppression, mass notification, utility monitoring and control (UMAC), airfield control, traffic signal control, vehicle barrier, security

Industrial Control Systems (ICS)

- Differ significantly from traditional administrative, mission support, and scientific data processing information systems
- "Operational Technology"
  - IT: Digital input = Digital output
  - OT: Digital input = Real World Change
- Unique characteristics
  - Extremely high availability, predictability, reliability
    - Driven by safety, operational, performance requirements
  - Need for real-time response

Then vs Now: What's Changed?

- Traditionally physically isolated from external and business networks
  - Hardware, software, communication protocols were proprietary



Source: Department of Homeland Security

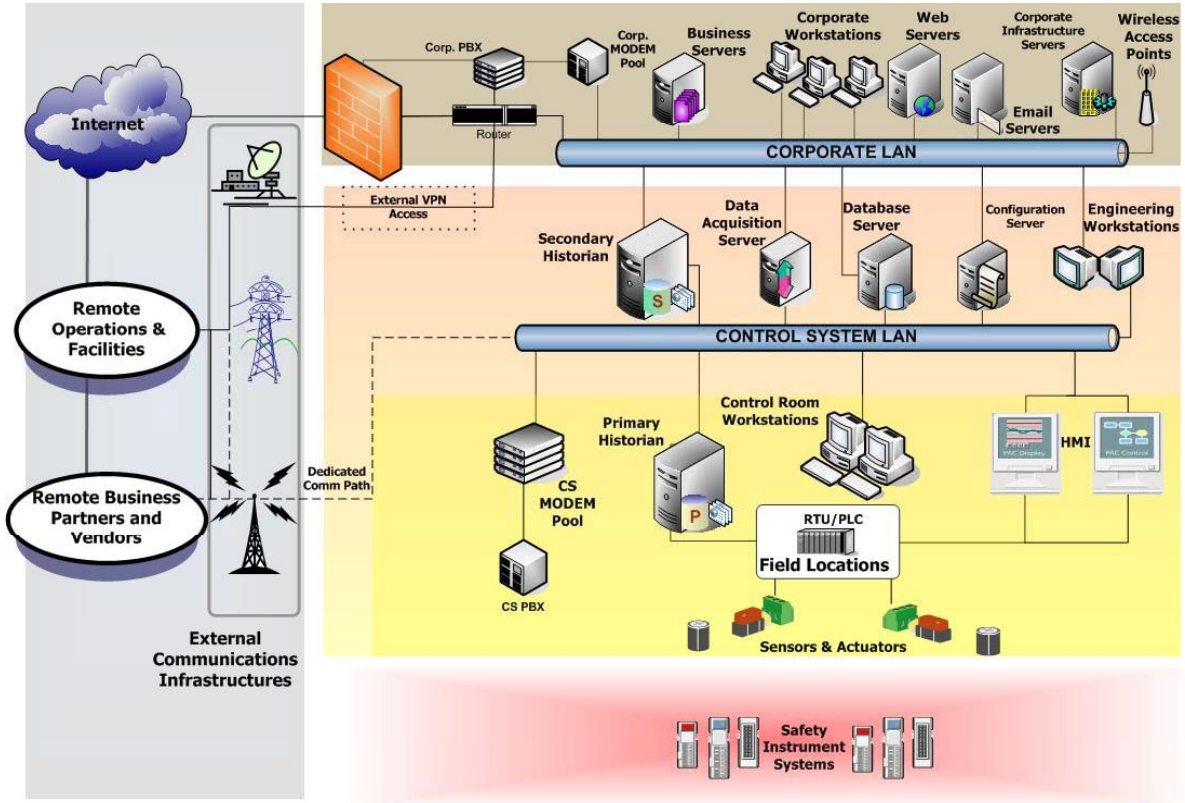
GovEnergy 2010

Then vs Now: What's Changed?

- Historically, OPSEC defined as level of reliability in operating safely and efficiently
- Total isolation from external networks meant threats were associated mostly with physical access to facility or plant floor
  - Limited authorization or security oversight required
- Operational commands, instructions, and data acquisition occurred in closed environment where all communications were trusted
  - Only authorized operators had access to the system

Then vs Now: What's Changed?

- Needs to enhance productivity and reduce costs by increasing integration of external, business, and control system networks



Source: Department of Homeland Security

GovEnergy 2010

Security Challenges

- By connecting networks and introducing IT components into the control domain:
  - Increasing dependency on automation
  - Insecure connectivity to external networks
  - Usage of technologies with known vulnerabilities, creating previously unseen cyber risk
  - Some technologies have limited internal security
    - Often only enabled if administrator is aware of capability (or if security does not impede process)
  - Protocols lack basic security functionality (e.g., authentication, authorization)
  - Open source information is available regarding ICS/BAS, their operations, and security vulnerabilities

Consideration of Domain Differences

SECURITY TOPIC	IT	ICS / BAS
Anti-virus & Mobile Code Countermeasures	Common; Widely Used	Uncommon; Difficult to Deploy
Support Technology Lifetime	3-5 Years	Up to 20 Years (or Longer)
Password Protection	Strong password capable/managed	Weak passwords; often never changed
Application of Patches	Regular/Scheduled	Slow (Vendor Specific)
Change Management	Regular/Scheduled	Legacy Based; Unsuitable for Modern Security
Time Critical Content	Delays are Generally Accepted	Critical Due to Safety
Availability	Delays are Generally Accepted	24x7x365 (Continuous)
Security Awareness	Good in Both Private and Public Sectors	Generally Poor Regarding Cyber Security
Security Testing/Audit	Scheduled and Mandated	Occasional Testing for Outages
Physical Security	Secure	Very Good, But Often Remote and Unmanned

Source: Idaho National Laboratory

Current DoD Policy

- Policy applies to "DoD Information Systems"
  - "set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information." (NSTISSI No. 4009, reference (c))
- DoDI 8500.2, Information Assurance (IA) Implementation
  - Establishes responsibilities and management structures for implementing IA
  - Decomposes "DoD Information Systems" into 4 categories: AIS Applications, Enclaves, Outsourced IT-Based Processes, Platform IT Interconnections (PITI)
  - Defines "Platform IT" (PIT) as systems essential to real-time mission performance
    - Includes ICS and building automation systems (BAS)
  - Places IA controls on PITI but not PIT
    - Connection is between PIT and Global Information Grid (GIG)
  - Places responsibility for addressing IA requirements with Heads of DoD Components
- DoDI 8510.01, DoD IA Certification and Accreditation Process (DIACAP), 2007
  - Manages implementation of IA capabilities and services and provides visibility of accreditation decisions regarding operation of DoD Information Systems (IS)

Information System Security Objectives

- Objectives for securing any DoD Information System
  - Confidentiality (i.e., unauthorized disclosure of info)
  - Integrity (i.e., unauthorized modification or destruction of info)
  - Availability (i.e., disruption of access to or use of info or an information system)
- Assess impacts for each objective based on <u>information system</u> and <u>information type</u>
  - Low (loss has limited adverse effect on operations, assets, or individuals)
  - Moderate (loss has serious adverse effect on operations, assets, or individuals)
  - High (loss has severe or catastrophic adverse effect on operations, assets, or individuals)

Assessment of Objectives and Impacts Defines Security Categorization (FIPS 199)

Drive to Change Policy

- Recognition in DoD that NIST's emerging Risk Management Framework (NIST SP 800-37) is better approach than DIACAP
- Recognition in DoD that ICS and BAS are evolving, increasingly exposed to threats and vulnerabilities
  - Must be brought under IA umbrella
- National Institute of Standards and Technology (NIST)
  - Developing technical guidance and baseline security safeguards to secure ICS/BAS (NIST SP 800-53 Rev 3)
  - Expected to significantly reduce risk of compromise and negative impacts to federal critical infrastructure
- FY10 NDAA, Subtitle D, Energy Security
  - Added Congressional report requirement to describe method to ensure DIACAP compliance on Energy Monitoring & Utility Control Systems

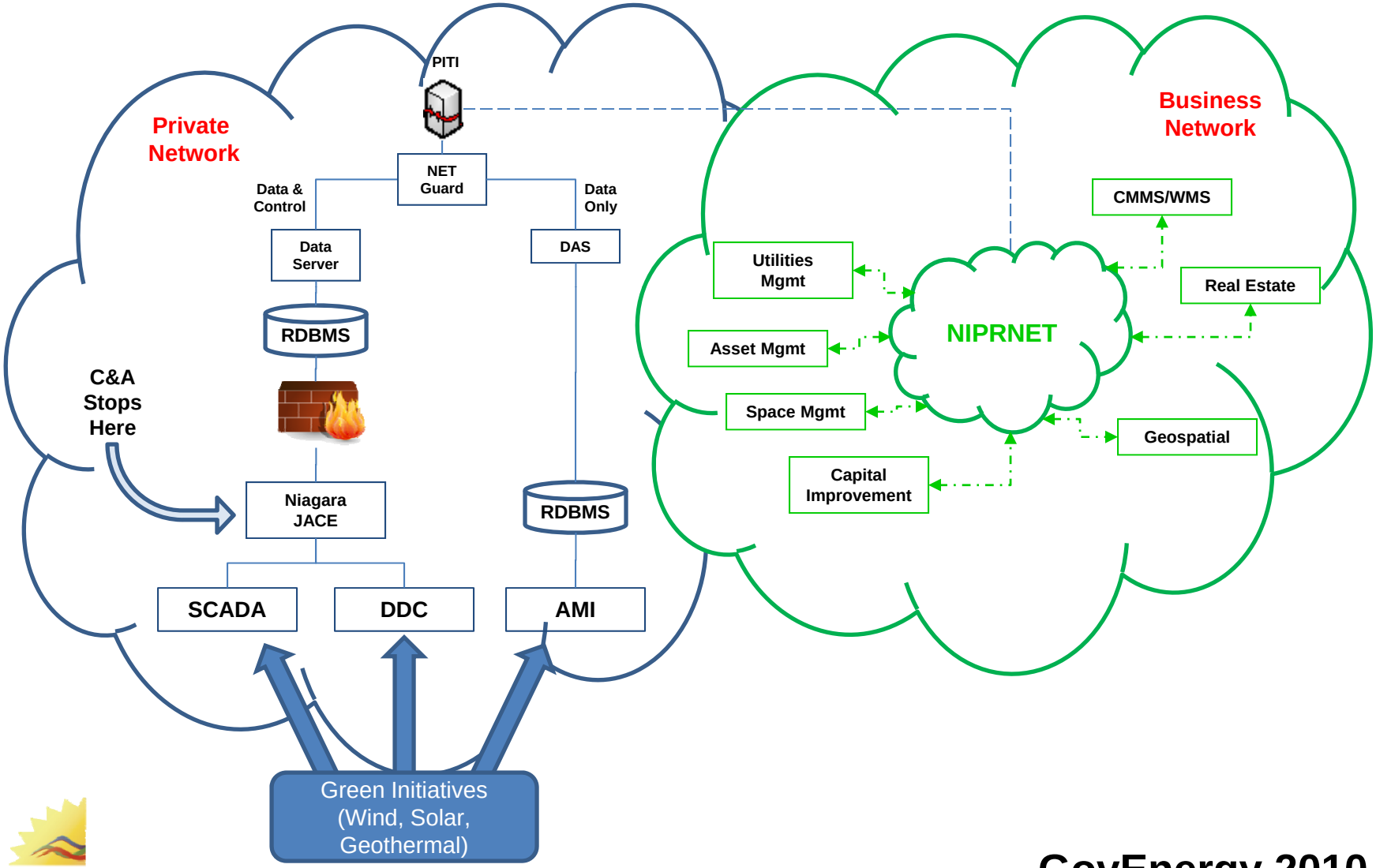
ICS/BAS Security Objectives

- Objectives for securing any ICS/BAS
  - Availability (i.e., disruption of access to or use of info or an information system)
  - Integrity (i.e., unauthorized modification or destruction of info)
  - Confidentiality (i.e., unauthorized disclosure of info)
- Plus:
  - Restrict logical access to control network and network activity
  - Restrict physical access to control network and devices
  - Protect individual control components from exploitation
  - Maintain functionality during adverse conditions
  - Plan for restoring ICS/BAS after incident

Next Policy Steps

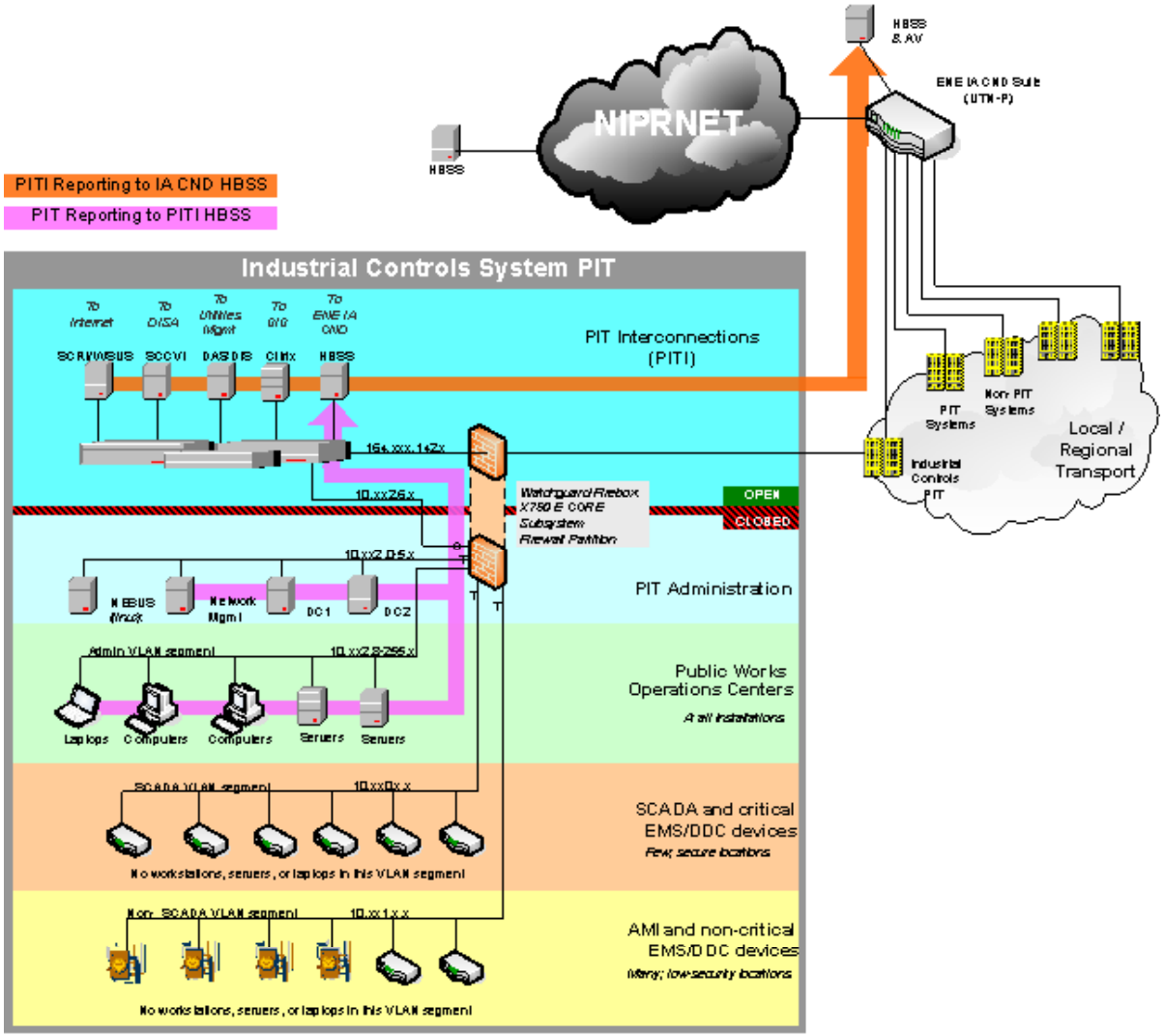
- DoD in process of migrating policy to use risk management framework and new NIST guidance
  - Intent is to separate ICS/BAS from Platform IT
- DoD Installations & Environment will be working with on development of new IA guidance specific to ICS/BAS
  - Define system boundaries, security categorization, control profile(s), preferred technical solutions, transition plan, compliance management and frequency
  - Identify functional community impacts
    - Costs, Designated Approval Authorities, Training, Personnel

Regional Solution #1 in Use



GovEnergy 2010

Regional Solution #2 in Use



Notes:
- PITI defined for individual systems
- PITI are the "open" side of a PIT, which are dual-homed with public and private IP addresses
- Devices on "closed" side have private IP addresses only
- ENE IA CND Suite is firewall between systems and NIPRNET
- PIT workstations and servers report to PITI HBSS
- PITI workstations and servers report to ENE IA CND Suite
- Orange and yellow blocks are Ethernet devices with embedded OS or no OS

GovEnergy 2010

Office of Deputy Undersecretary of Defense
Installations & Environment (I&E) Business Enterprise Integration
Stacey S. Tyley
Smart Installations Program Manager

QUESTIONS?