Challenges in Implementing an Agency-wide Advanced Metering System: IT Security and Support Needs

Interagency Sustainability Working Group
January 12, 2017

GSA

Karen Curran, PBS Office of Facilities Management
Sandy Shadchehr, GSA IT

Agenda

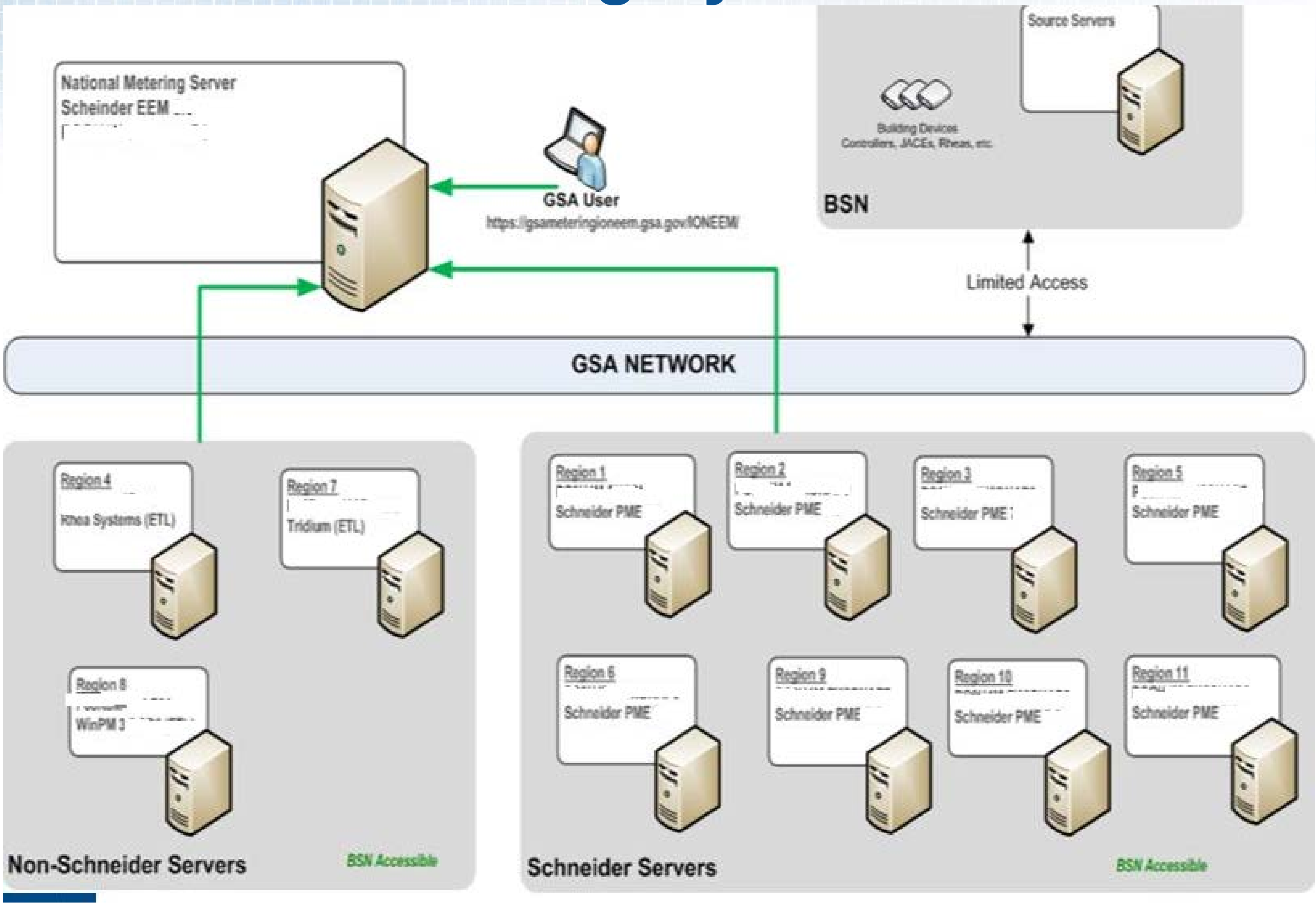
- GSA Advanced Metering Status
- Architecture
- Background on integrating Adv Metering System to the GSA network
- Best Practices
- Inception to Activation of New Meters on the GSA Network
- Device Scanning Process
- Wireless
- Documents
- Challenges – Program Wide
- Support Structure
- Key takeaways

GSA’s Advanced Metering Program – Status

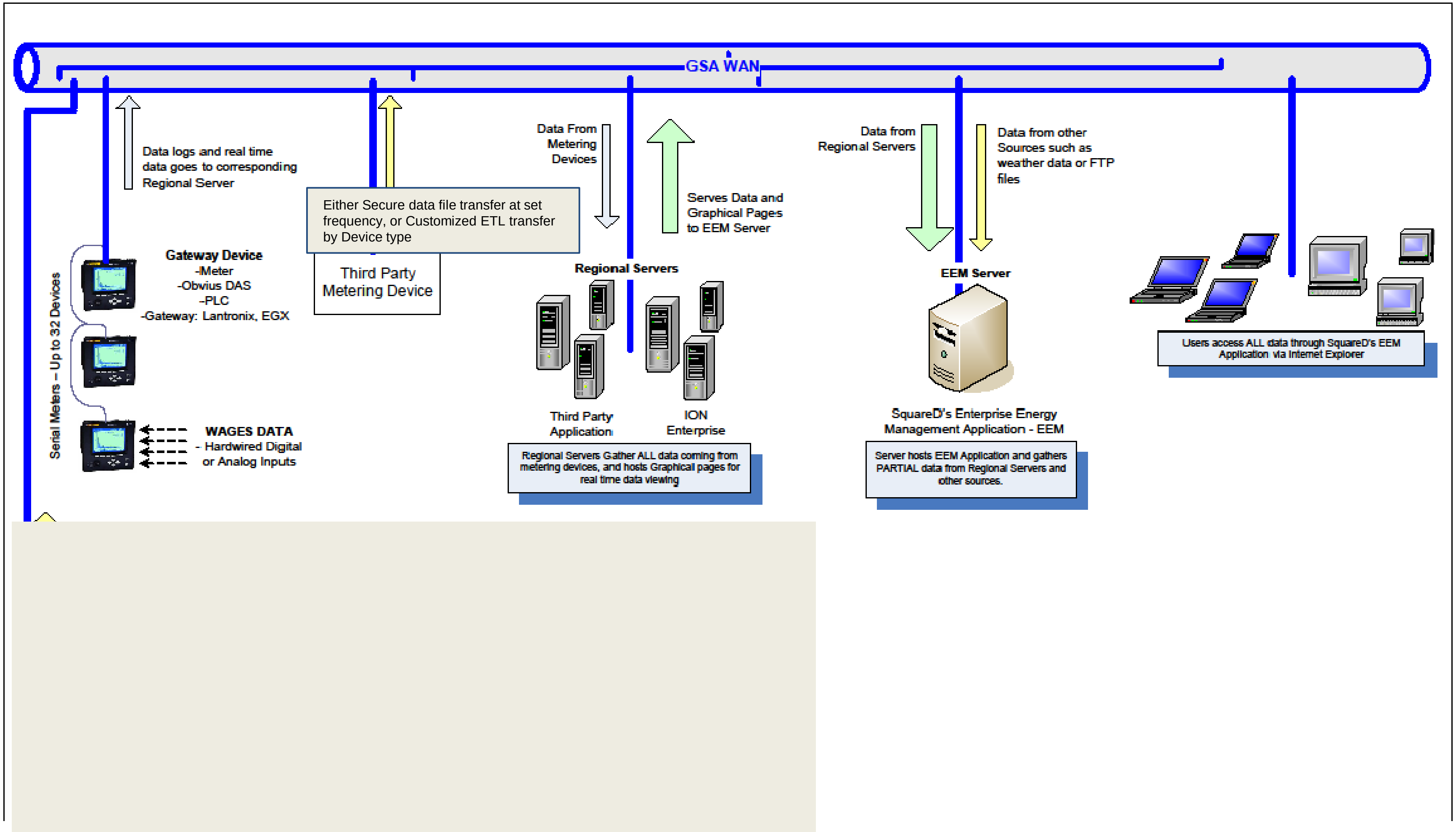
- Inventory (Approx 40 Unique Devices/Vendors- IP Enabled 6 Unique ETLs)
  - Just under 700 IP Enabled Devices
  - Total of 5,300 Enabled Sources Devices
  - 40,000 Source Measurement Pairs
- Energy/ Water – Advanced Metering
- On-Going Efforts
  - New sites
  - Finishing up Gas/Steam/ Water
  - Sub-Metering (tenant/ Equipment/ Specific loads)

GSA (Owned)	Adv Meter
Electric	90.43%
Gas	73.33%
Steam	83.68%
Water	47.68%

Advanced Metering System Architecture



Data Flow From Device to User Interface



GSA WAN

Serial Meters – Up to 32 Devices

Data logs and real time data goes to corresponding Regional Server

Gateway Device
-Meter
-Obvius DAS
-PLC
-Gateway: Lantronix, EGX

WAGES DATA
- Hardwired Digital or Analog Inputs

Either Secure data file transfer at set frequency, or Customized ETL transfer by Device type

Third Party Metering Device

Data From Metering Devices

Serves Data and Graphical Pages to EEM Server

Regional Servers

Third Party Application

ION Enterprise

Regional Servers Gather ALL data coming from metering devices, and hosts Graphical pages for real time data viewing

Data from Regional Servers

Data from other Sources such as weather data or FTP files

EEM Server

SquareD's Enterprise Energy Management Application - EEM

Server hosts EEM Application and gathers PARTIAL data from Regional Servers and other sources.

Users access ALL data through SquareD's EEM Application via Internet Explorer

Background

- **2005-2007** - Legislative directives that mandated advance metering requirements for the Federal agencies. Executive Order 13423, Section 103 of the Energy Policy Act of 2005 and Section 434 (b) of the Energy Independence Security Act of 2007

- **July 2008** - PBS CIO issued the "Advanced Metering System Implementation Guide", providing direction on connectivity options for Advanced Metering Systems

- **March 2011** - GSA issued policy signed by CIO, PBS Facility Management Assistant Commissioners and PBS Design and Construction Assistant Commissioners - "Technology Policy for PBS-Owned Buildings Monitoring and Control Systems" - all Advanced meters must be behind the GSA firewall

- **April 2011** - GSA publishes "The Building Technologies Technical Reference Guide (BTTRG), a formalized guidance related to the technical integration of building monitoring and control systems (BMC) to the GSA network

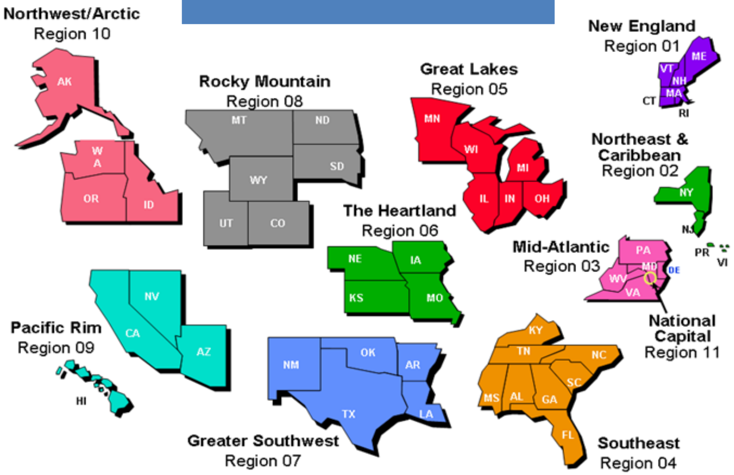
- **June 2011**- GSA establishes process for FISMA compliance and interconnectivity, **Building Technologies Tech Reference Guide.**

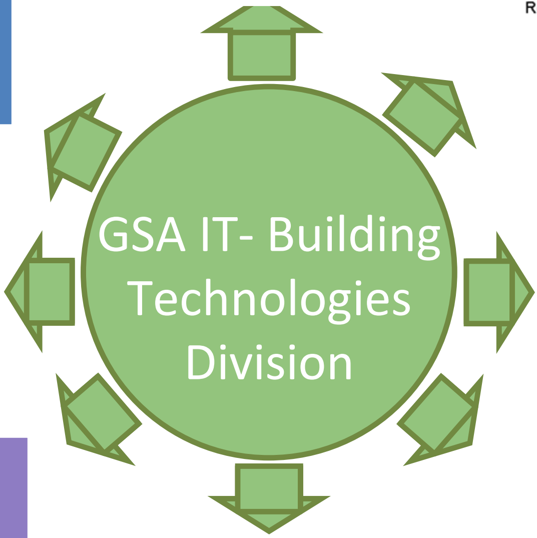
GSA Best Practices

- Business line and GSA IT collaborate on integration efforts
- Quarterly meetings with major manufacturers
- Streamlining the IT Security Building Device Assessment process
  - Criteria established by NIST SP 800-53 Rev 4 controls standards and using NIST SP 800- 82 to assist in tailoring to address BMC system
  - Guidelines on Assessment process, including SLAs
    - Security Assessment Reports (SAR)
    - Remediation
  - Bi-Weekly meetings with key stakeholders to discuss prioritization and status
- IT Security requirements referenced in SOW for all new Adv Metering projects

Cross-Functional Collaboration

GSA Regions





GSA IT- Building Technologies Division

GSA IT -Server and BAS support

PBS - Design & Construction

Industry

PBS- Facilities Management (Smart Buildings and Energy Metering Division)

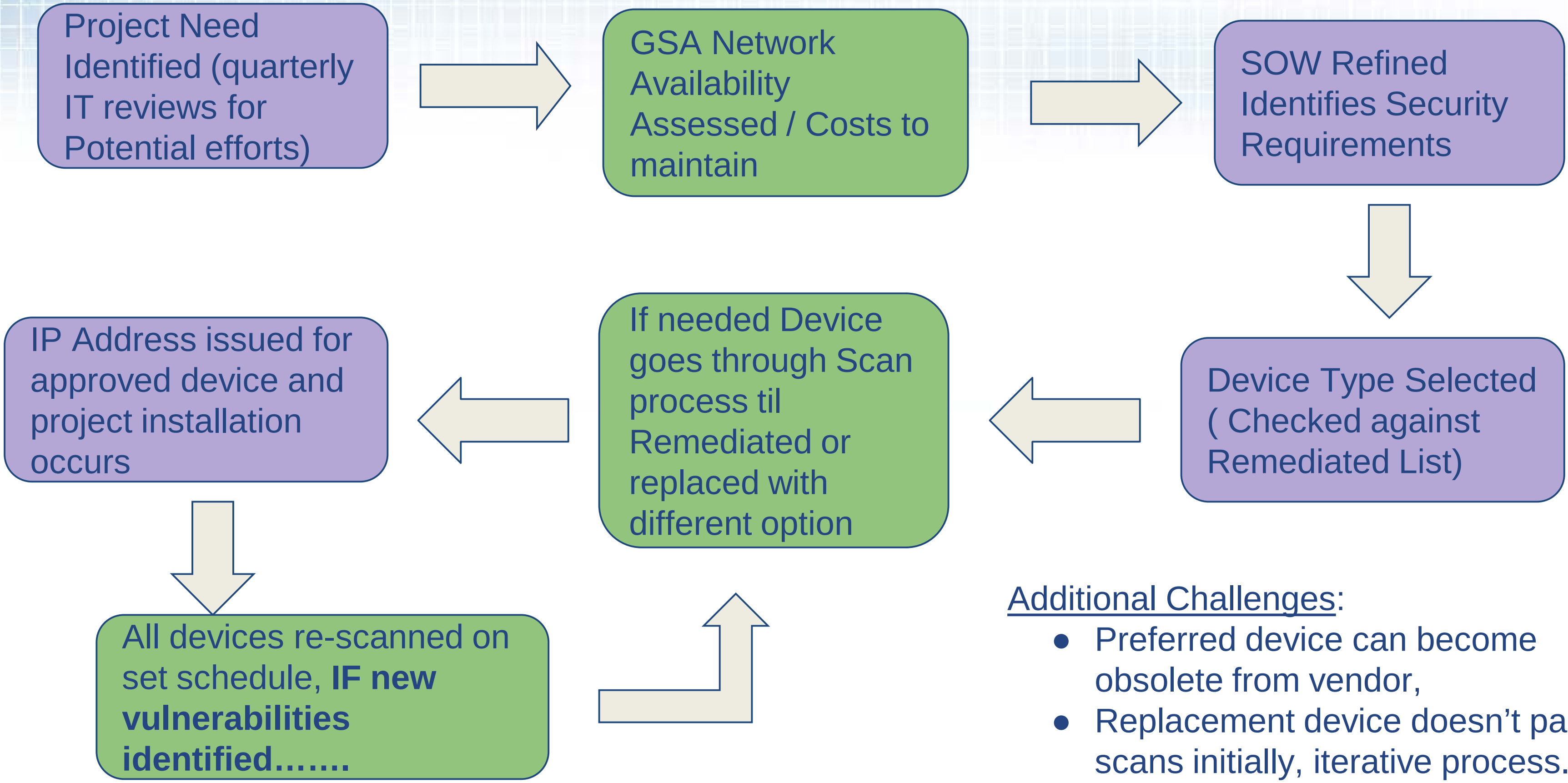
GSA-IT Network Operations

GSA IT Security

GSA IT - Local Support

Metering O&M

Inception to Activation of New Meters on the GSA Network



Project Need Identified (quarterly IT reviews for Potential efforts)

GSA Network Availability Assessed / Costs to maintain

SOW Refined Identifies Security Requirements

Device Type Selected (Checked against Remediated List)

If needed Device goes through Scan process til Remediated or replaced with different option

IP Address issued for approved device and project installation occurs

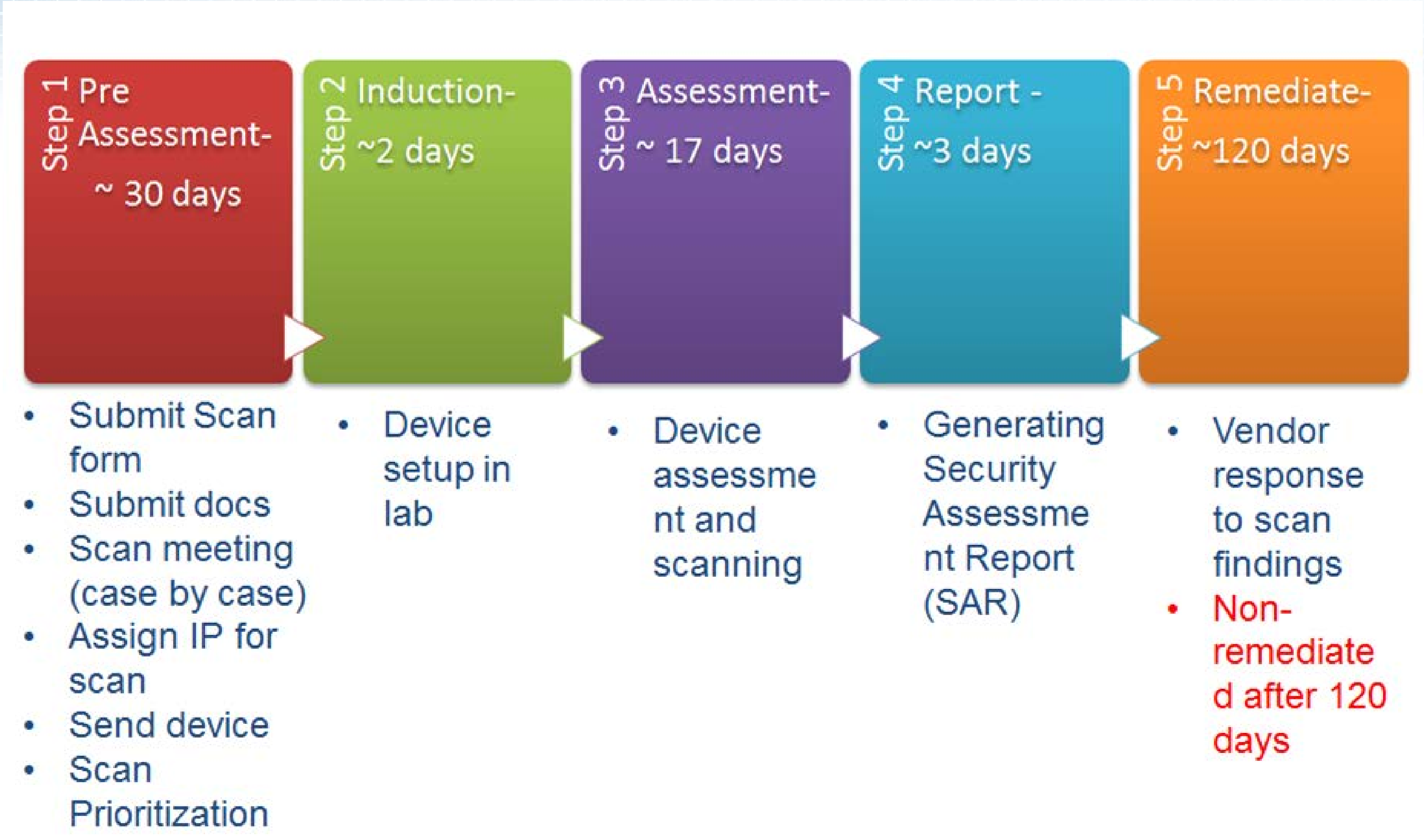
All devices re-scanned on set schedule, **IF new vulnerabilities identified…….**

Additional Challenges:

- Preferred device can become obsolete from vendor,
- Replacement device doesn’t pass scans initially, iterative process.

- ❖ IT Budget covers cost of maintaining GSA network at sites, so iterative discussion needed to stay ahead of budget cycle to cover costs. Definition of “Practicable” impacted by budget and costs
- ❖ Collaborative effort between Business Line and IT to tweak scope to ensure vendors know what is required.
- ❖ Devices need to be re-reviewed/assessed after 3 years

BMC Device Assessment Process



Step 1 Pre Assessment- ~ 30 days

- Submit Scan form
- Submit docs
- Scan meeting (case by case)
- Assign IP for scan
- Send device
- Scan Prioritization

Step 2 Induction- ~2 days

- Device setup in lab

Step 3 Assessment- ~ 17 days

- Device assessment and scanning

Step 4 Report - ~3 days

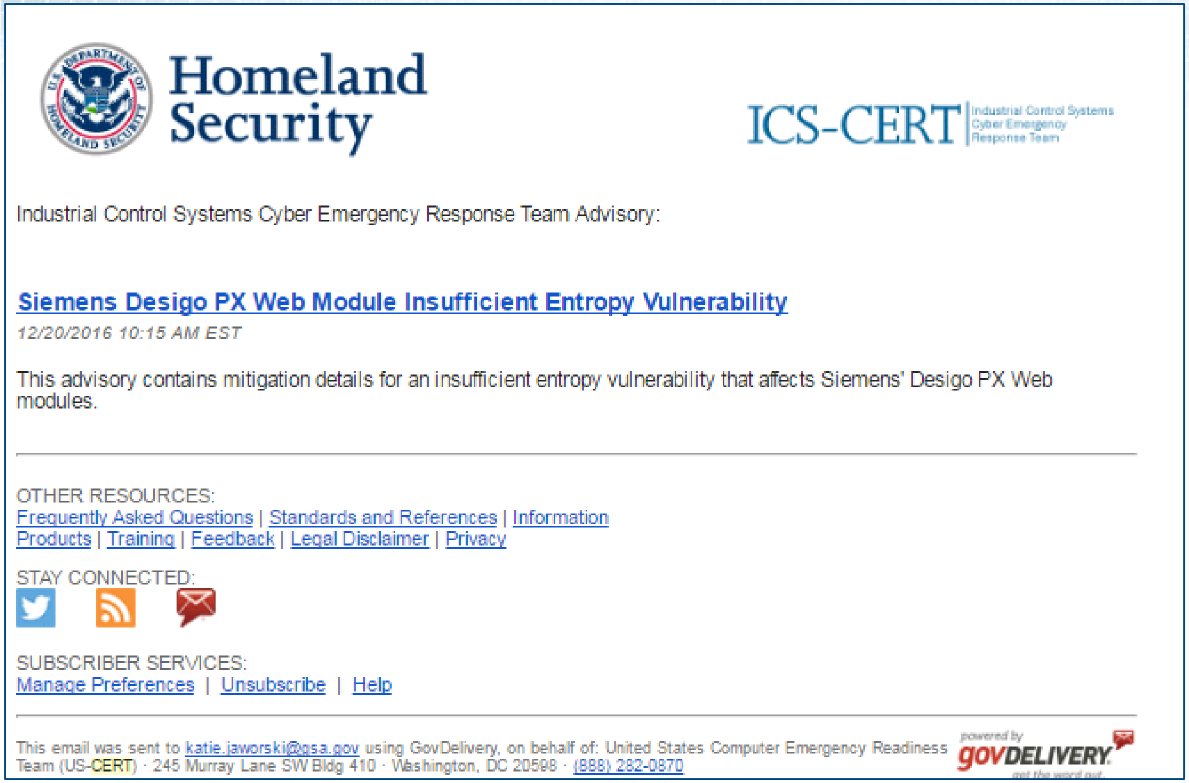
- Generating Security Assessment Report (SAR)

Step 5 Remediate- ~120 days

- Vendor response to scan findings
- Non-remediated after 120 days

Note: All timelines are an estimate and depend on vendor participation

Notification for New Vulnerabilities & EOL Notices



Homeland Security

ICS-CERT Industrial Control Systems Cyber Emergency Response Team

Industrial Control Systems Cyber Emergency Response Team Advisory:

Siemens Desigo PX Web Module Insufficient Entropy Vulnerability

12/20/2016 10:15 AM EST

This advisory contains mitigation details for an insufficient entropy vulnerability that affects Siemens' Desigo PX Web modules.

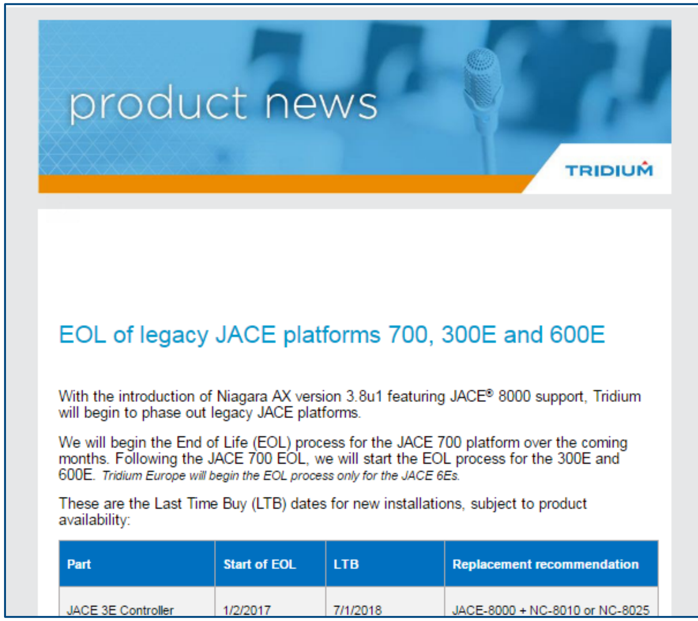
OTHER RESOURCES:
Frequently Asked Questions | Standards and References | Information
Products | Training | Feedback | Legal Disclaimer | Privacy

STAY CONNECTED:

SUBSCRIBER SERVICES:
Manage Preferences | Unsubscribe | Help

This email was sent to katie.jaworski@gsa.gov using GovDelivery, on behalf of: United States Computer Emergency Readiness Team (US-CERT) · 245 Murray Lane SW Bldg 410 · Washington, DC 20598 · (888) 282-0870

powered by govDELIVERY get the word out



EOL of legacy JACE platforms 700, 300E and 600E

With the introduction of Niagara AX version 3.8u1 featuring JACE® 8000 support, Tridium will begin to phase out legacy JACE platforms.

We will begin the End of Life (EOL) process for the JACE 700 platform over the coming months. Following the JACE 700 EOL, we will start the EOL process for the 300E and 600E. *Tridium Europe will begin the EOL process only for the JACE 6Es.*

These are the Last Time Buy (LTB) dates for new installations, subject to product availability:

Part	Start of EOL	LTB	Replacement recommendation
JACE 3E Controller	1/2/2017	7/1/2018	JACE-8000 + NC-8010 or NC-8025

Wireless

- Wireless technology is constantly changing. GSA is currently working on updating wireless policy.
- General guidance:
  - All wireless solutions need to adhere to FISMA and GSA policy
  - All wireless solutions are required to be evaluated and approved by GSA IT Security, in advance of any implementation.
    - Wireless solutions, regardless of whether they are IP, will need to be reviewed by GSA IT Security
    - Adheres to NIST FIPS 140-2 Encryption Standards to include FIPS approved encryption protocols, e.g., TLS 1.1 or higher and FIPS approved ciphers, e.g., Advanced Encryption Standard (AES)
  - All wireless solutions must adhere to the "2100.2B CIO P GSA Wireless Local Area Network (LAN) Security" guide

Documents

- NIST 800-82 rev 2
- GSA documents:
    - Building Technologies Technical Ref Guide
    - IT Security Procedure Guide – Device Assessment Process
    - GSA order 2100.1J GSA Information Technology (IT) Security Policy
    - IT Security Procedural Guide: Key Management CIO-IT Security-09- 43
    - 2100.2B CIO P GSA Wireless Local Area Network (LAN) Security guide.
    - Top 10 Most Common Vulnerabilities
    - GSA IT Security Procedural Guide: SSL TLS Implementation Guide - CIO-IT Security 14-69

Please note: Prior approval is needed from GSA IT Security Office before internal documents are shared with other agencies*

Challenges

- Reaching every Project Manager
- Vendor cooperation and responsiveness
- User community - perception that IT security adds problems
- IT Security Compliance - evolving tech and security risks
- Cost/resource reality check
- Support resources needed
- **Competition- creates diverse architecture, at the same tim**e doesn't afford us the ability to standardize on IT support and security configuration which results in greater costs and complexities in implementation
- Accurate inventory tracking

GSA Advanced Metering Support Structure

- Daily Source Activity Report (Great Tool) – Identify when meters aren’t reporting
- 2 Support Contracts for OFM - Office of Facilities Mgmt
  - National Adv Metering Support Contract - Troubleshooting
    - Dedicated email distro for users to submit issues
    - Dedicated queue on Enterprise GSA IT helpdesk
      - Troubleshooting /Triage of new tickets
      - Route ticket to SE/ NetOps/ Further review
      - Goal to make sure nothing gets lost
      - Monitor time to resolve / most common issues
      - Create log/ monitor tickets
      - Separate component for Repair Needs
    - SE - ION EEM Support – Application Support
      - Schneider application specific issues

Key Takeaways

- Education of Vendors as to what is Required and expected
- Not always a quick process, not going away, so working together only path to success
  Identify key stakeholders and establish process and working relationship as soon as possible
- On-going costs must be included in analysis… NOT cost effective or “Practicable” to adv meter everything everywhere!
- On-Going Support is a MUST HAVE and worth every penny!
- Every new meter must be supported and has a cost associated with it, so smart decision on where and what to meter can lead to great efficiencies in energy and water

Use of Metering Data(Bldg Perspective)

Energy billing & Procurement

- Verifying utility bills
  Bill Auditing
- Tenant energy use (sub metering)
- Identifying best rates
- Participating in demand response programs

Optimize/Review performance

- Diagnose equipment & systems operations
- RETUNING
- Benchmark utility use
- ID potential projects
- ID power quality problems
- Modelling (more adv users)
- On-Site Generation monitoring

Verify project performance

- **Promote** energy awareness

Demand Response Programs
Monitor **actions** when response needed

- Measure results
- ID potential savings from DR

Use of Metering Data (Agency – Enterprise View)

•Energy Procurement
•Load Aggregation
•Load Factor
•Participating in demand response programs

•Benchmarking
•Baseline comparisons
•Start-Up Comparisons
•Energy/Water intensity
•Trends across similar building types

Verification for Reporting Mandates

Promote energy awareness & Sharing Lessons Learned

How We Are ACTUALLY Using the Data

- Engaging (Partnering) O&M Staff/ Energy Teams
  - Reviewing trends daily / periodically – asking questions, Why ? Should this be occurring?
  - Finding Leaks (Water)
  - Modifying our O&M Specs to require review of data
  - Provides oversight to our O&M, not possible before, especially in remote sites

- Using Report Subscription Capability
  - O&M Staff/ Senior Mgmt

- Making Models to validate suspicions

- Re-Tuning
  - Proper analysis of utility and interval meter data can result in the identification of significant energy savings opportunities and possibly improve overall building operations.
  - Using it with First Fuel Software (Rapid Bldg Assessment)

karen.curran@gsa.gov