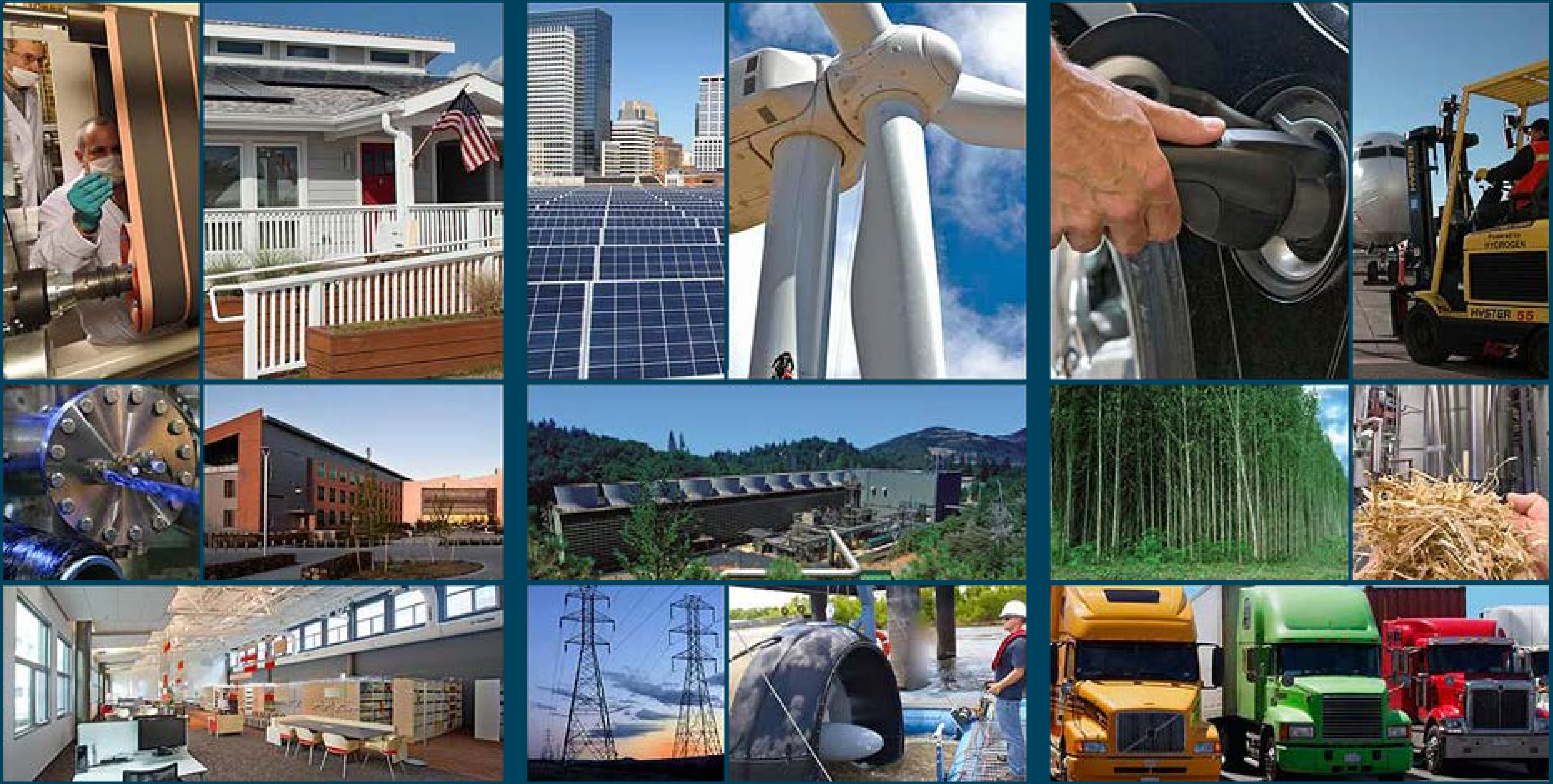
Overview of the BTO Cybersecurity Related Buildings Project

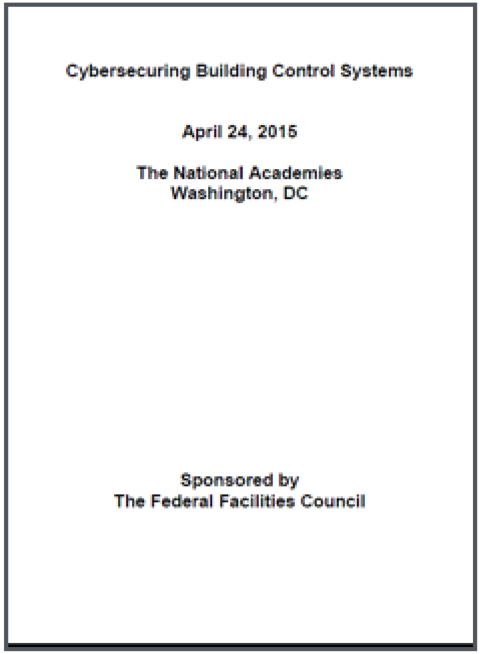


U.S. DEPARTMENT OF ENERGY

Energy Efficiency & Renewable Energy

January 12, 2017

Increasing Cyber Vulnerability & DOE Buildings Role



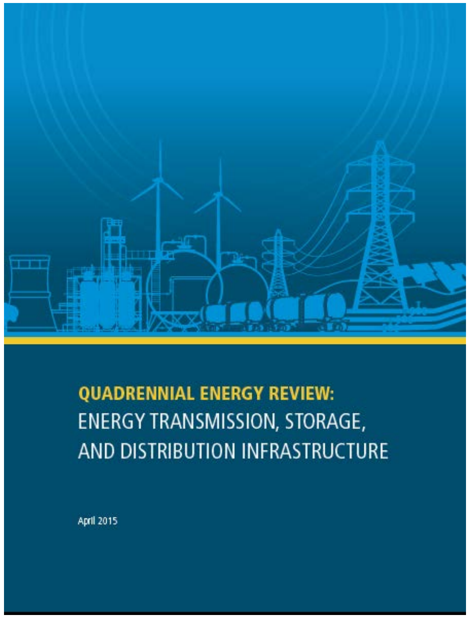
Cybersecuring Building Control Systems

April 24, 2015

The National Academies
Washington, DC

Sponsored by
The Federal Facilities Council

“**The nation's buildings are increasingly relying on building control systems with embedded communications technology and many enabled via the Internet**. These systems provide critical services that allow a building to meet the functional and operational needs of building occupants…but can also be easy targets for hackers and people with malicious intent... **As these systems are becoming more connected, so is their vulnerability to potential cyber-attacks.”**

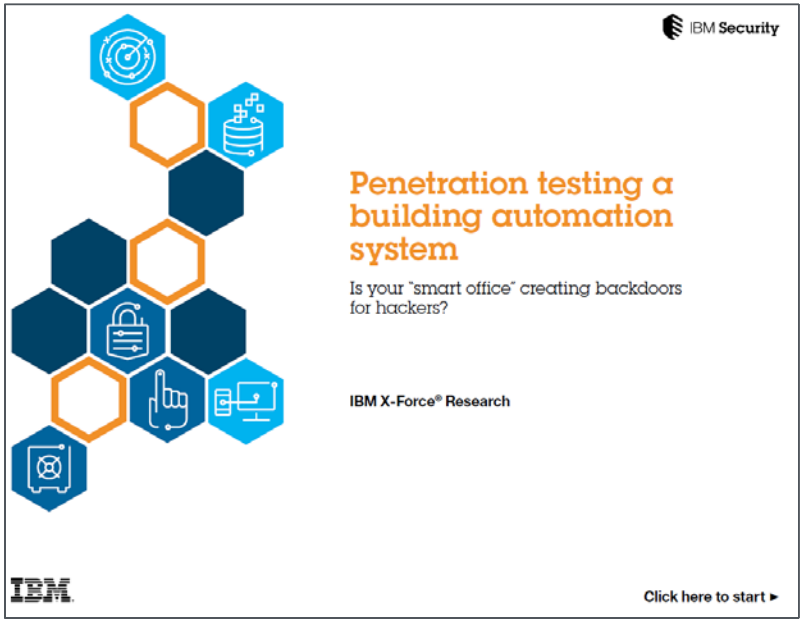


QUADRENNIAL ENERGY REVIEW:
ENERGY TRANSMISSION, STORAGE,
AND DISTRIBUTION INFRASTRUCTURE

April 2015

“While DHS coordinates the overall Federal effort to promote the security and resilience of the nation’s critical infrastructure, in accordance with Presidential Policy Directive-21, **DOE serves as the day-to-day Federal interface for sector-specific activities** to improve security and resilience in the energy sector.”

CASE STUDY: IBM Building Control System Vulnerabilities



IBM Security

Penetration testing a building automation system

Is your "smart office" creating backdoors for hackers?

IBM X-Force® Research

IBM

Click here to start ►

http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WGL03110USEN

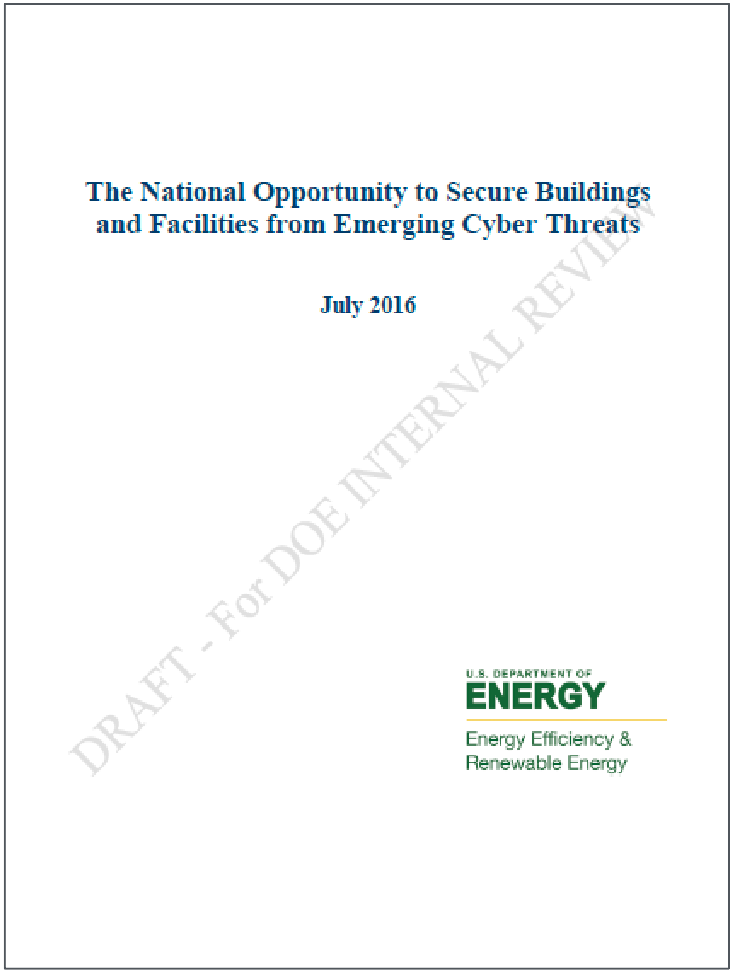
IBM Ethical Hacking team "conducted an assessment of a BAS that controlled sensors & thermostats in a commercial office. Working with system operator & building management, **we tested & found several areas of concern in BAS architecture that could allow a malicious attacker not only to take control of an individual building system, but also to then gain access to a central server**, operated by system operator, which **could extend control to several other geographically dispersed buildings**."

PNNL Review

- Represents a fairly typical case
- If facility running BACnet or Modbus, not much they can do in terms of security other than isolating their facilities network & controlling access.
  - BACnet actually has a security protocol but infrequently implemented.
- If connection done right, risk may be minimal, but this level of cybersecurity requires dedicated & expert IT staff -- which most buildings don't have.

Draft White Paper on Buildings Cybersecurity & *Illustrative* Stakeholder Questions

1. What are most significant cyber threats & vulnerabilities to buildings & facilities?
2. What activities or measures are businesses & others currently implementing or pursuing to enhance the cybersecurity of connected appliances, equipment, & other systems, devices, & controls in buildings?
3. **How can the potential cyber threats, vulnerabilities, & impacts to buildings & facilities be better quantified to manage risk?**
4. Given diversity of buildings, how can "appropriate" levels of cybersecurity risk management be defined so that building owners & operators can specify & deploy the necessary mitigations?
5. How can the costs associated with "appropriate" levels of protection be minimized?
6. **Over the next 5 years, what are the highest-priority activities for defining, implementing, and/or strengthening cybersecurity in buildings?**



The National Opportunity to Secure Buildings and Facilities from Emerging Cyber Threats

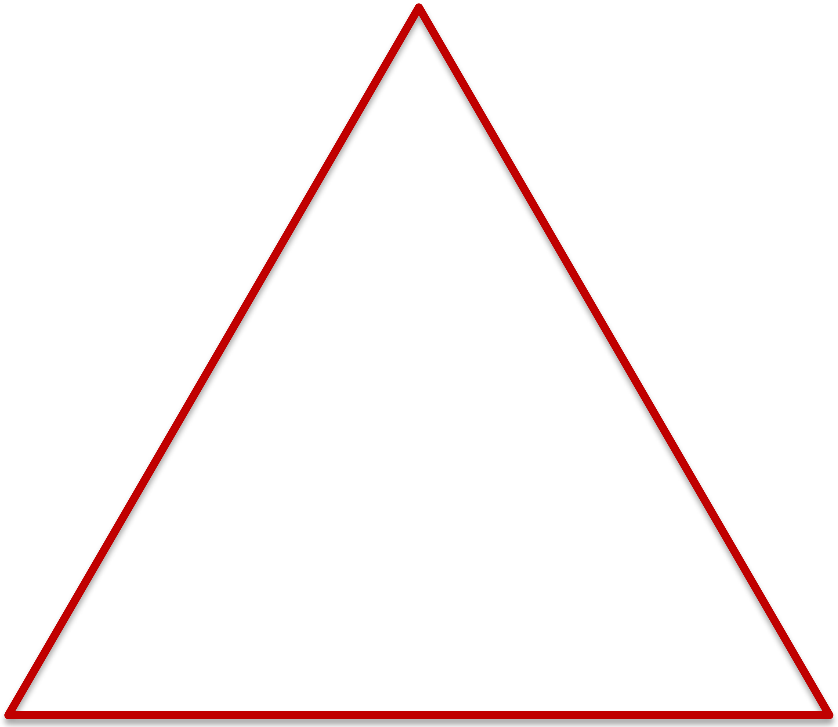
July 2016

U.S. DEPARTMENT OF ENERGY

Energy Efficiency & Renewable Energy

BTO Perspective: Cyber Security needed for Smart Buildings & Connected Equipment

Smart Buildings

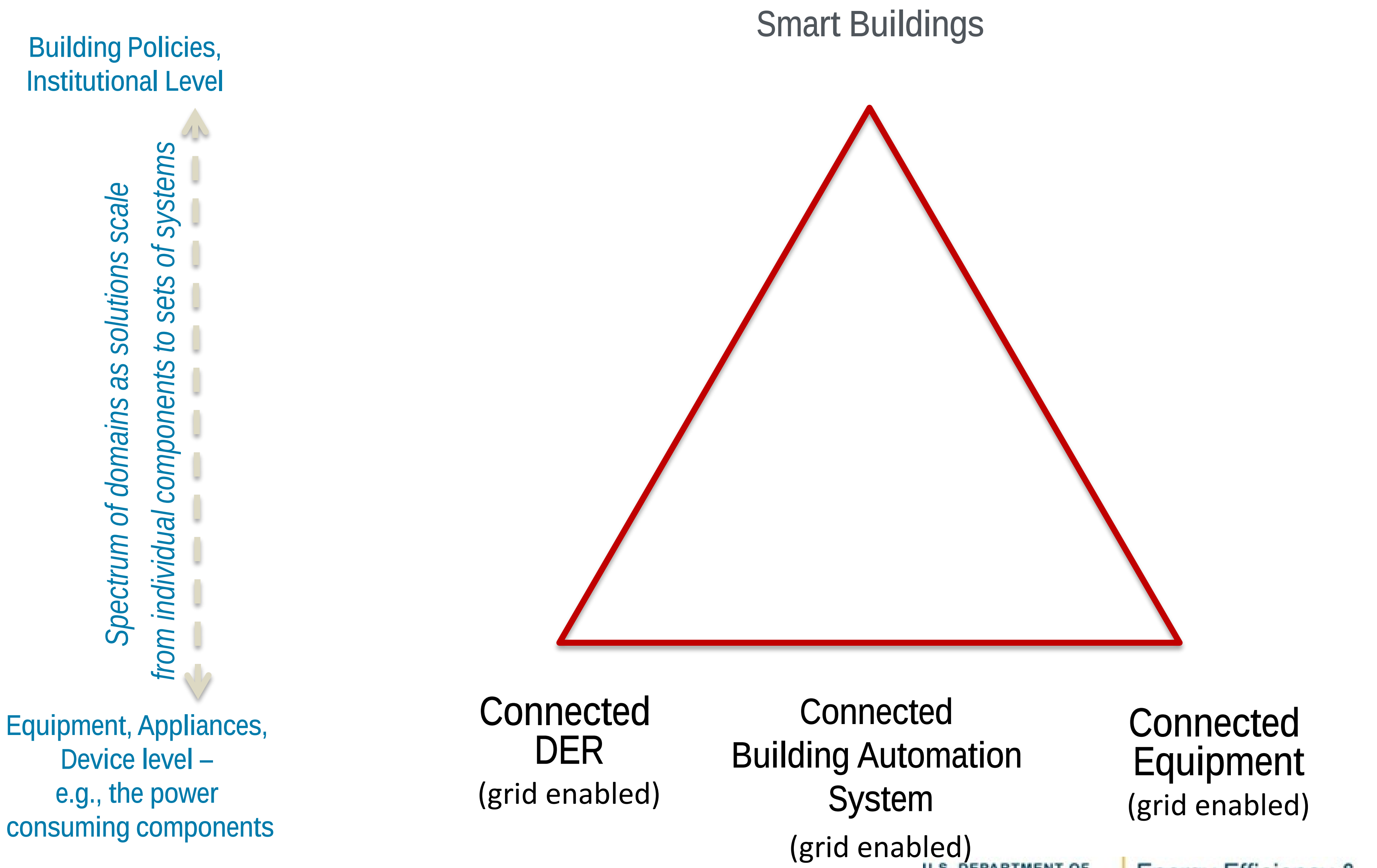


Connected DER
(grid enabled)

Connected Building Automation System
(grid enabled)

Connected Equipment
(grid enabled)

BTO Perspective: Cyber Security needed for Smart Buildings & Connected Equipment



Smart Buildings

Building Policies, Institutional Level

Spectrum of domains as solutions scale from individual components to sets of systems

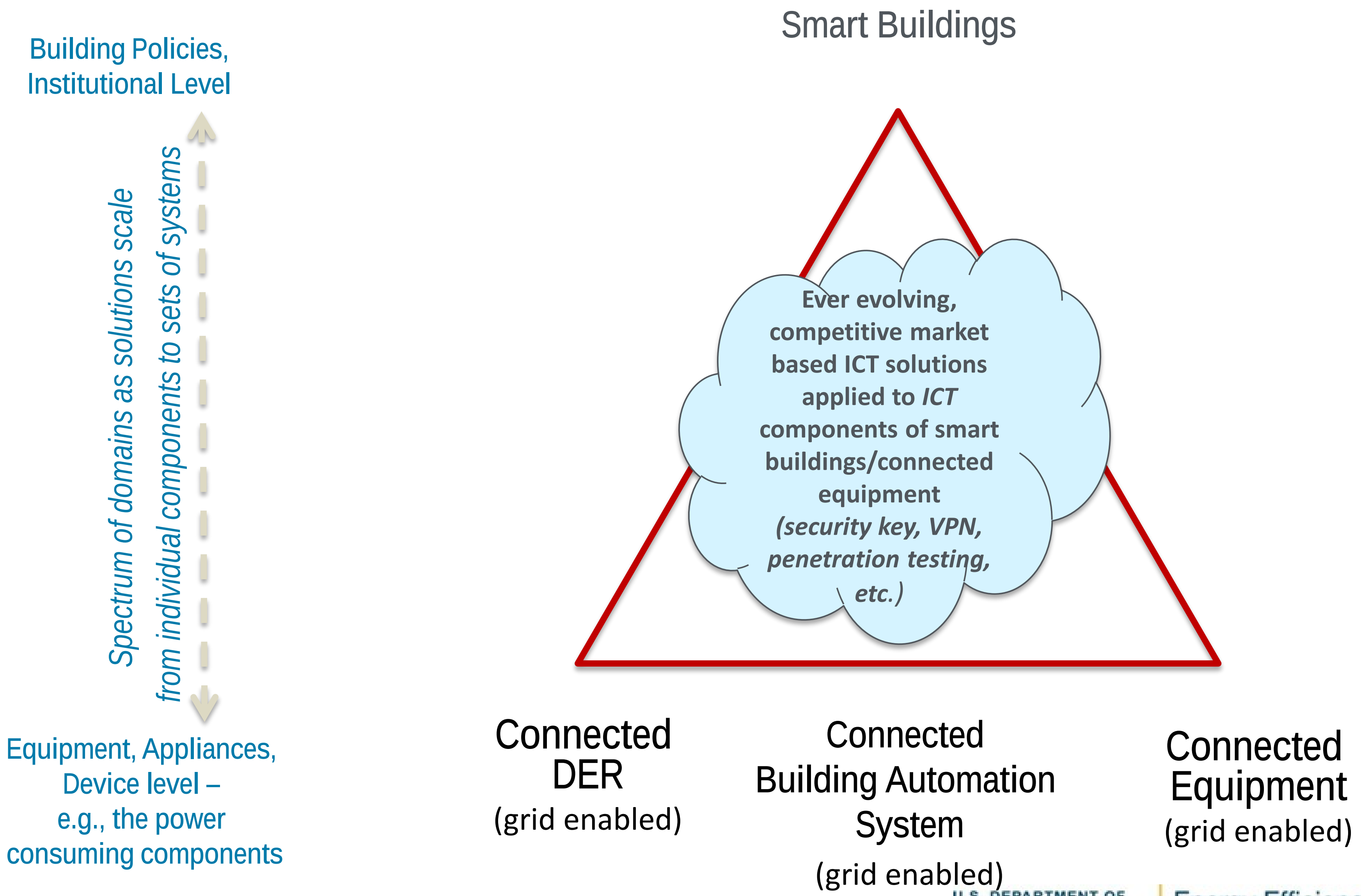
Equipment, Appliances, Device level – e.g., the power consuming components

Connected DER (grid enabled)

Connected Building Automation System (grid enabled)

Connected Equipment (grid enabled)

BTO Perspective: Cyber Security needed for Smart Buildings & Connected Equipment



Smart Buildings

Building Policies, Institutional Level

Spectrum of domains as solutions scale from individual components to sets of systems

Equipment, Appliances, Device level – e.g., the power consuming components

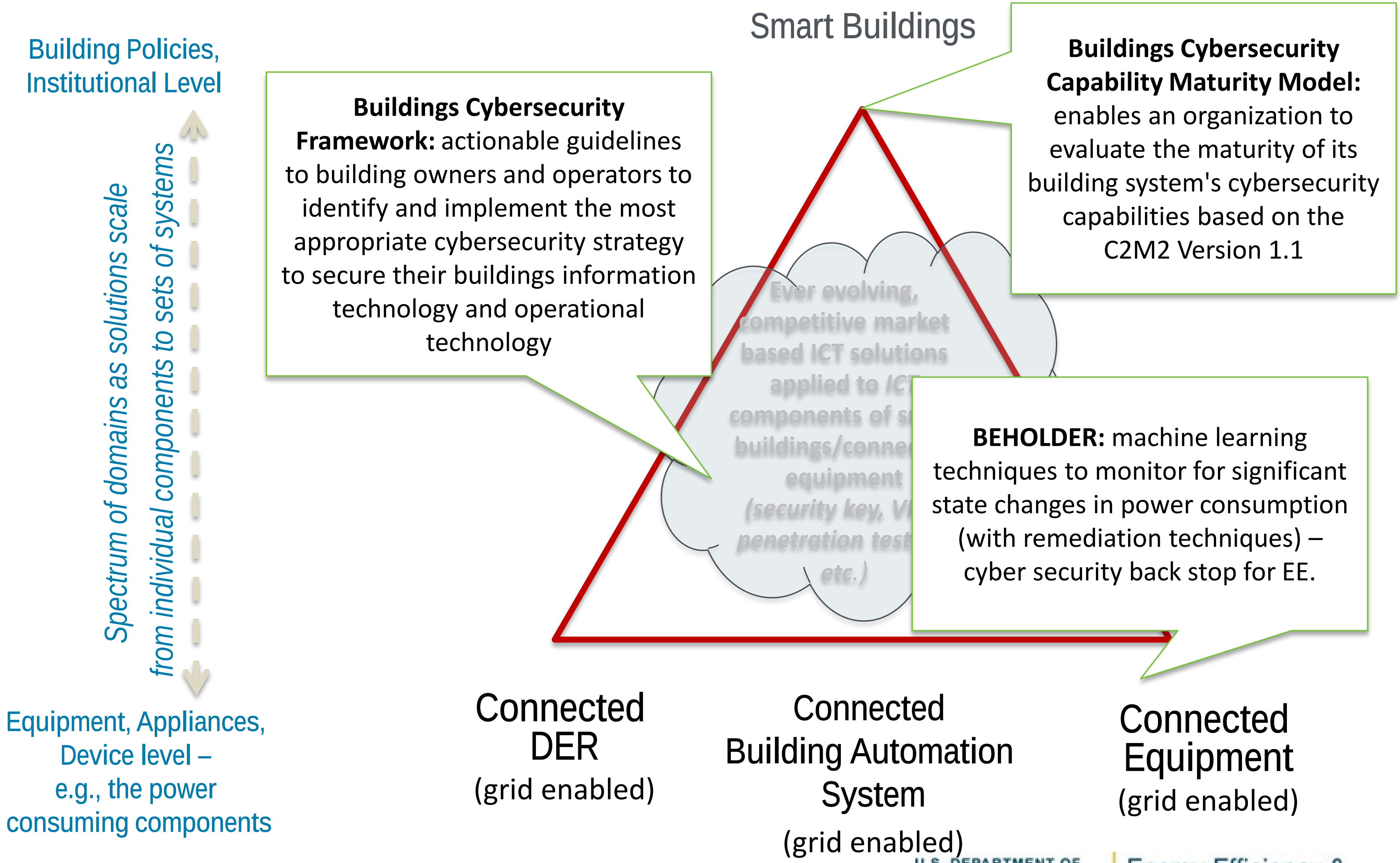
Ever evolving, competitive market based ICT solutions applied to *ICT* components of smart buildings/connected equipment *(security key, VPN, penetration testing, etc.)*

Connected DER (grid enabled)

Connected Building Automation System (grid enabled)

Connected Equipment (grid enabled)

BTO Perspective: Cyber Security needed for Smart Buildings & Connected Equipment



Building Policies, Institutional Level

Spectrum of domains as solutions scale from individual components to sets of systems

Equipment, Appliances, Device level – e.g., the power consuming components

Smart Buildings

Buildings Cybersecurity Framework: actionable guidelines to building owners and operators to identify and implement the most appropriate cybersecurity strategy to secure their buildings information technology and operational technology

Buildings Cybersecurity Capability Maturity Model: enables an organization to evaluate the maturity of its building system's cybersecurity capabilities based on the C2M2 Version 1.1

Ever evolving, competitive market based ICT solutions applied to *ICT* components of s buildings/conne equipment *(security key, V penetration test etc.)*

BEHOLDER: machine learning techniques to monitor for significant state changes in power consumption (with remediation techniques) – cyber security back stop for EE.

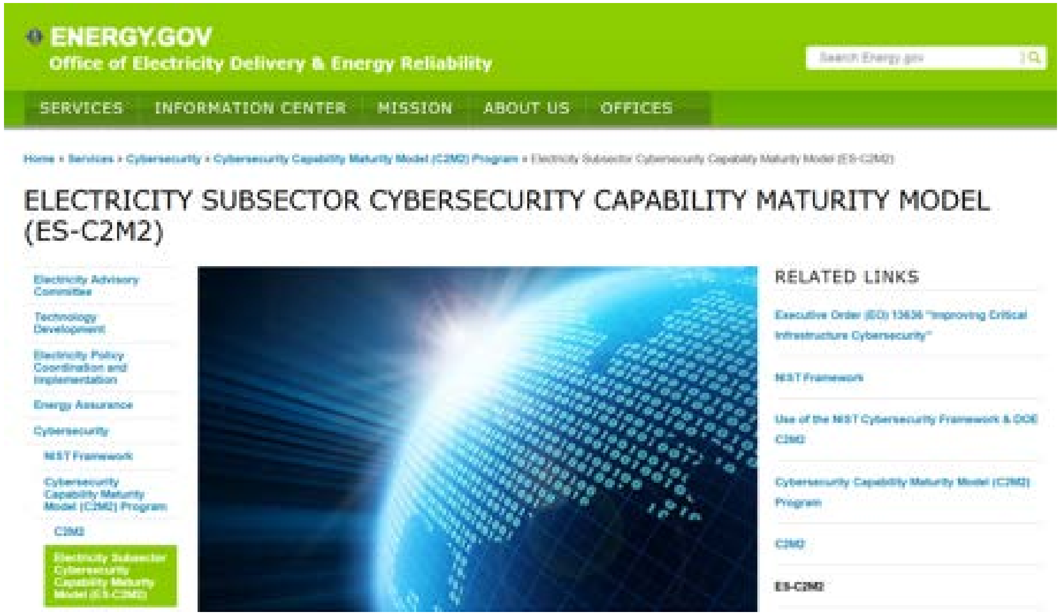
Connected DER (grid enabled)

Connected Building Automation System (grid enabled)

Connected Equipment (grid enabled)

U.S. DEPARTMENT OF ENERGY | Energy Efficiency & Renewable Energy

Leveraging DOE Office of Electricity's Investments in Cyber Maturity Models for FEMP/BTO



ENERGY.GOV
Office of Electricity Delivery & Energy Reliability

Home › Services › Cybersecurity › Cybersecurity Capability Maturity Model (C2M2) Program › Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)

ELECTRICITY SUBSECTOR CYBERSECURITY CAPABILITY MATURITY MODEL (ES-C2M2)

- Electricity Advisory Committee
- Technology Development
- Electricity Policy Coordination and Implementation
- Energy Assurance
- Cybersecurity
  - NIST Framework
  - Cybersecurity Capability Maturity Model (C2M2) Program
    - C2M2
    - Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)

RELATED LINKS

- Executive Order (EO) 13636 "Improving Critical Infrastructure Cybersecurity"
- NIST Framework
- Use of the NIST Cybersecurity Framework & DOE C2M2
- Cybersecurity Capability Maturity Model (C2M2) Program
- C2M2
- ES-C2M2

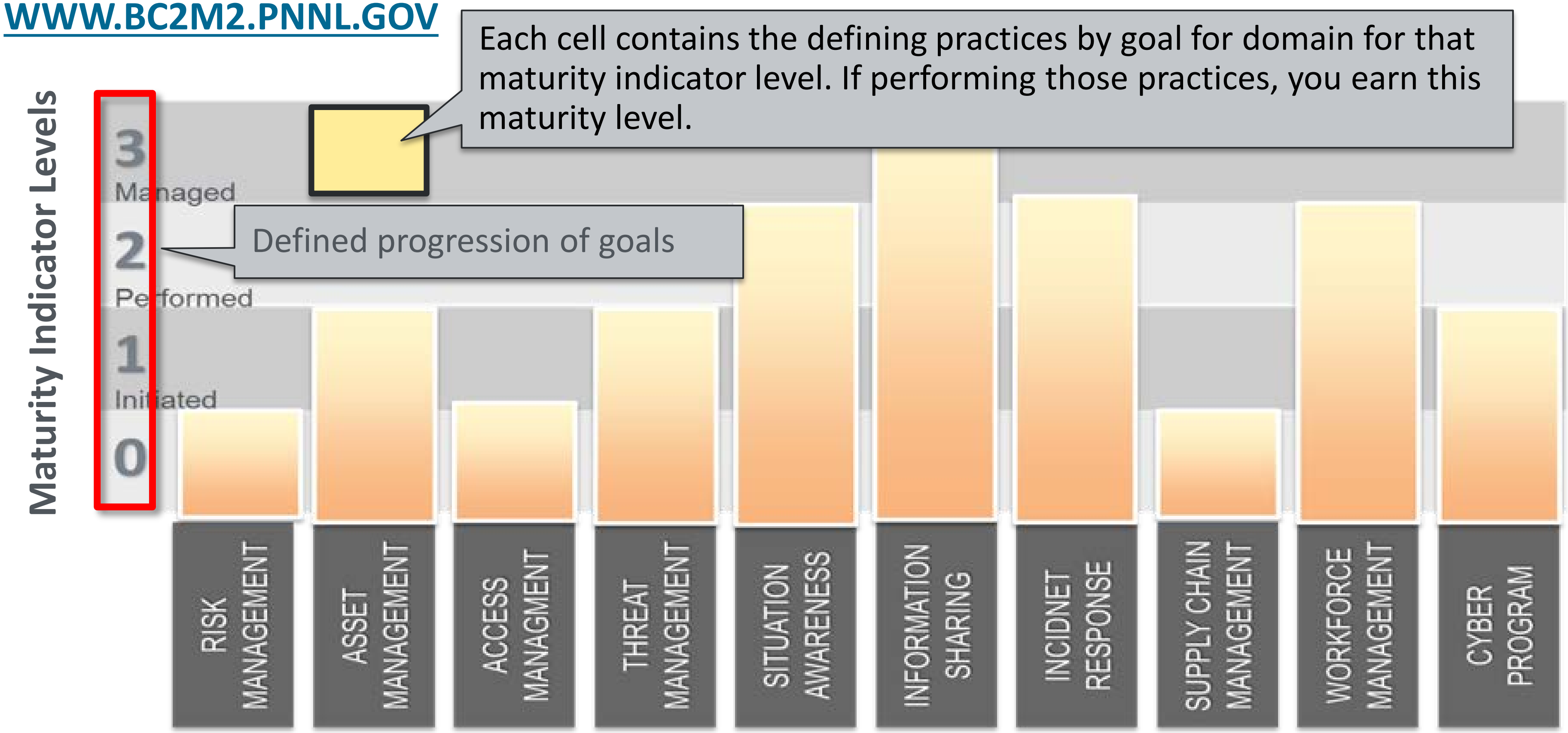
Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) established as result of Administration's efforts to improve elec. sector cybersecurity capabilities, to understand cybersecurity posture of energy sector. ES-C2M2 includes the core C2M2 and additional reference material and implementation guidance specifically tailored for elec. sector.

What is a "maturity model" and why do we need them?

- Many organizations have trouble explaining what is exactly wrong and what they want done – **discussing symptoms not root causes**
- Many diagnostic tools exist to help identify problem areas - SWOT analysis, benchmarks, check lists, etc.
- Another tool is **maturity model** which gauges the client's relative "maturity" in a number of areas and points out the areas of improvement.

Buildings Cybersecurity Maturity Model (B-C2M2)

WWW.BC2M2.PNNL.GOV



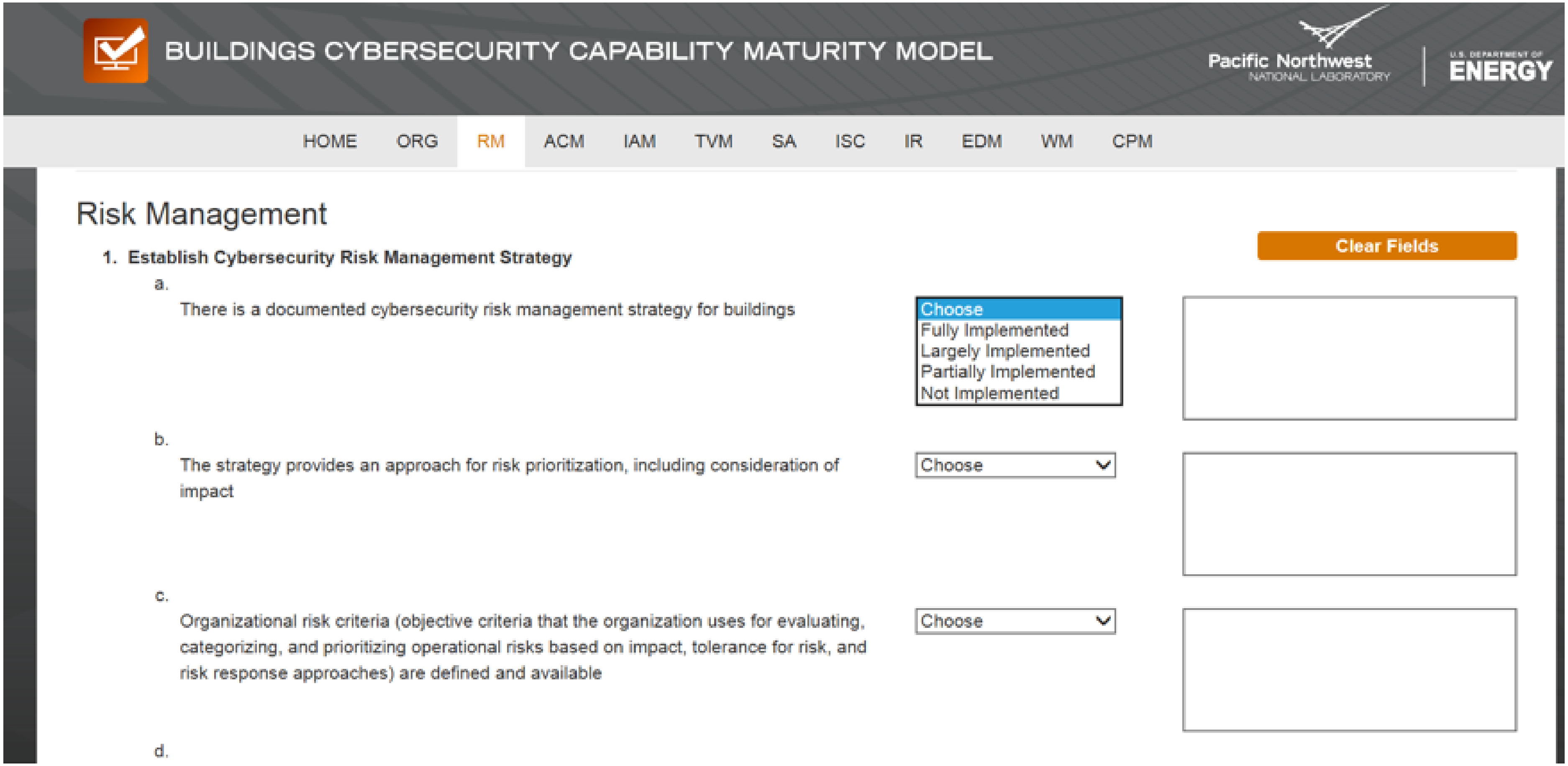
Each cell contains the defining practices by goal for domain for that maturity indicator level. If performing those practices, you earn this maturity level.

Defined progression of goals

Other Maturity Models

- Cybersecurity Capability Maturity Model (C2M2) (DOE Office of Electricity)
  - Electricity Subsector C2M2
  - Oil/Nat. Gas Subsector C2M2
- Smart Grid Interoperability Maturity Model (Gridwise Architecture Council)

B-C2M2 – Risk Management Screen Shot



Risk Management

1. **Establish Cybersecurity Risk Management Strategy**

a.

There is a documented cybersecurity risk management strategy for buildings

b.

The strategy provides an approach for risk prioritization, including consideration of impact

c.

Organizational risk criteria (objective criteria that the organization uses for evaluating, categorizing, and prioritizing operational risks based on impact, tolerance for risk, and risk response approaches) are defined and available

d.

What the B-C2M2 is and is not

B-C2M2…

- ✓ Is completely voluntary
- ✓ Evaluates the maturity of an organization’s cybersecurity capabilities
- ✓ Focuses on the programmatic structure
- ✓ Provides descriptive and flexible guidance
- ✓ Publicly available
- ✓ Designed to take 2 hours or less

B-C2M2 IS NOT…

- ✕ Required or mandated
- ✕ Guidance for implementing specific security controls
- ✕ An audit, controls assessment, or a penetration test.
- ✕ Intended to replace other cybersecurity-related activities, programs, processes, or approaches.
- ✕ DOE collecting data

B-C2M2 Pilots and Lessons Learned

PNNL conducted **pilot assessments at five sites**

- Large lab facility
- Municipal building
- University campus
- Community college campus
- Federal Agency campus

Lessons Learned

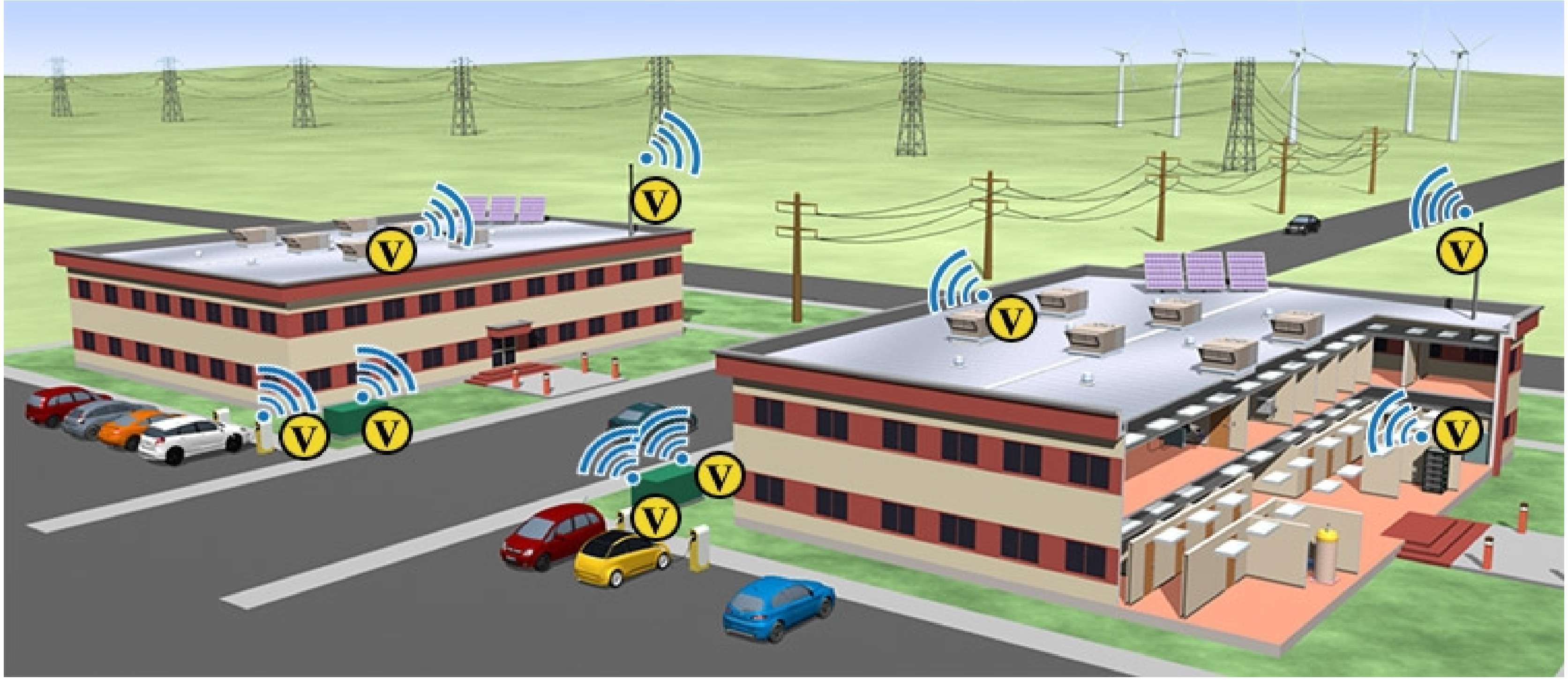
- Considerable range in maturity of cybersecurity programs
- Lack of any formal risk assessment & mgmt. program for building control systems
  - Much being done right, though ad-hoc
- Mature IT cyber program helps, but does not address all risks
- B-C2M2 questions raised awareness. Often heard “I hadn’t thought of that – I think I should start paying more attention to…”

Cyber Security for Appliances (ORNL)

Model #: RF28K9580SR

- **Objective**
  - Develop low-level intrusion detection and remediation techniques for enhancing cyber security of connected appliances
    - ✓ Detect the presence of cyber-events (i.e., malware) by monitoring the ***power consumption*** of a smart refrigerator
- **Problem**
  - Malware avoids detection by rewriting portions of itself
  - Signature based detection methods are not efficient enough
    - ✓ Only effective against known malware
    - ✓ Costly to implement in terms of downtime and system resources
    - ✓ Ineffective against polymorphic malware

EERE RD Supporting Development Of Cybersecure Controls Platform



VOLTTRON is **an application platform** (e.g., Android, iOS) for distributed sensing/control applications. Attributes include:

- Open-source, flexible, modular and scalable
- **Built in features to streamline app developmen**t
- **Secure communication** (e.g., security libraries/cryptography)
- Platform services

For More Information:
http://bgintegration.pnnl.gov/volttron.asp and volttron@pnnl.gov