U.S. DEPARTMENT OF ENERGY

Cryptographic Standards Acceptance and the User Experience

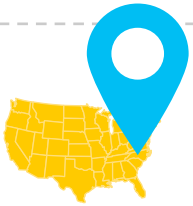
ICMC U30a Keynote: Friday, May 19, 2017

Gordon Bass, Director
Cybersecurity Operations Office
Office of the CIO
U.S. Department of Energy

DOE Cyber Footprint – Enterprise-wide

Locations

14th Largest agency by size



97 entities across in **27** states

People

Approximately **108,400** people supporting the DOE Enterprise

14,915 *Federal employees & support service contractors*

93,485 *M&O's & other contractors*

User Accounts

225,029
Total Accounts

17,965
Privileged

207,064
Standard

16,715 *Federal Mobile Devices*

297,538
Unclassified Endpoints

68,618
Federal

228,920
M&O & other contractors

197 Open Data Centers *(Unclassified)*

39 *Federal*

158 *M&O & other contractors*

112 *High Value Assets*
50+ HVAs which contain PII

15
Federal IT Service Providers

Average Helpdesk Ticket Volume

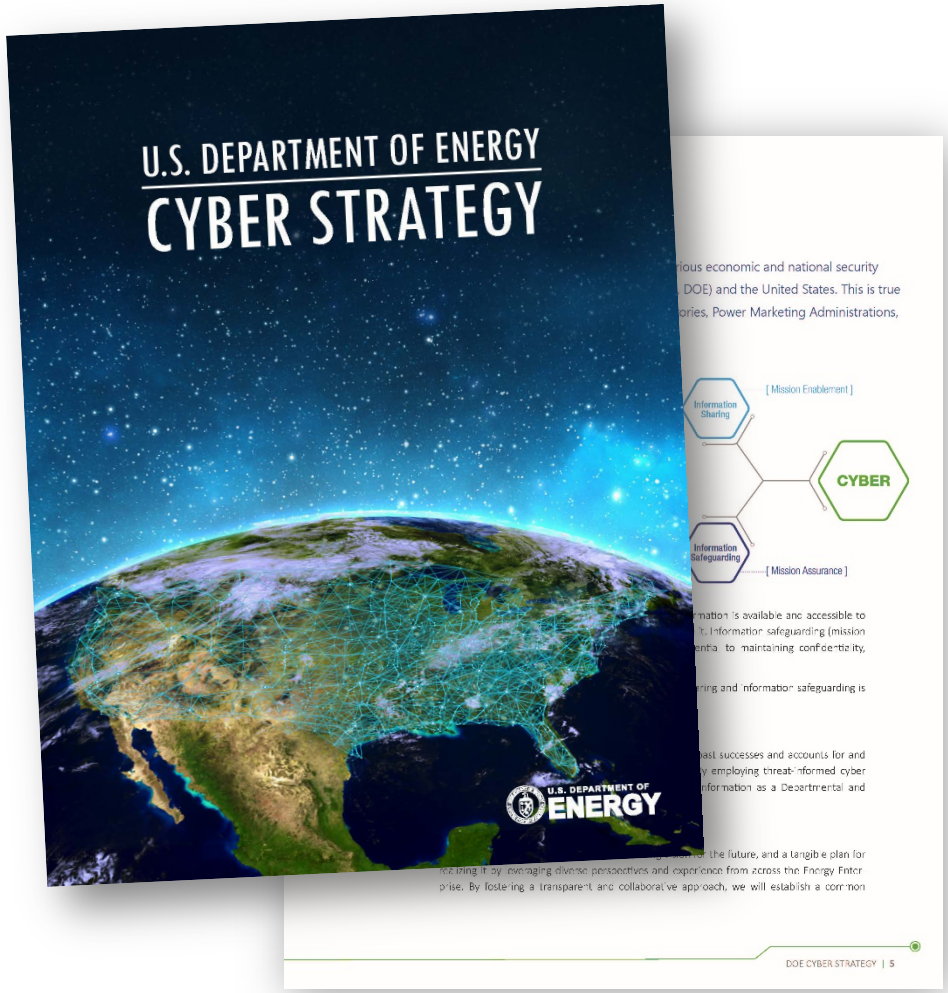
24,679 per month

DOE Cyber Strategy

The Strategy sets forth DOE's enduring commitment to securing our cyber assets.

Implementing this Strategy will enhance our ability to protect our critical infrastructure and to identify and report cyber incidents so that we can respond promptly and manage their consequences.

Available at: ***http://energy.gov/cio/downloads/doe-cyber-strategy-0***



OCIO - Cybersecurity Operations Office

- **Mission:** Manage Cybersecurity Risk for the OCIO and other DOE Organizations through performance of Assessments and Authorizations (A&A)
- **Process:** Federal Information Security Management Act (FISMA)
  - Augmented by Additional Directives and Programs from:
    - OMB: Managing Information as a Strategic Resource (Circular A-130)
    - NIST: Risk Management Framework (RMF), Federal Information Processing Standards (FIPS), Cybersecurity Framework
    - GSA: FedRAMP
    - DHS: Continuous Diagnostics and Mitigation (CDM)
    - DOE: Cyber Security Program (Order 205.1B, Change 3)

A Typical User Problem: Noncompliant Products

- **Business Goal:** Acquire and Authorize a New System
- **Challenge:** The proposed system does not meet one or more key security requirements *(FIPS 140-2, for example)*
- **Solution:** There is often no clear and easy solution
  - Option 1: Reject the proposed system, based on failure to meet security requirements
  - Option 2: Acquire the proposed system, based on the need for the functionality it offers and accept the risk associated with the non-compliant aspects
  - Which is the better option – 1 or 2?
    - How much time and effort does it take to decide?
    - What mitigations may need to be implemented to manage the cyber risk to an acceptable level, and at what cost?

The User Dilemma: Authorize the System?

- **Answer (Part 1):** Maybe – It Depends! Is the security gap a deviation from a *"Standard"* or a *"Guideline?"*
- **NIST Standards and Guidelines:** FISMA directs the Secretary of Commerce to prescribe Standards and Guidelines
  - Standards (FIPSs) are compulsory and binding for agencies
  - Guidelines (SPs) are recommendations and guidance
- **Answer (Part 2):** A User (Agency Authorizing Official) *Cannot* accept risk and authorize a system that deviates from a Standard (ex: FIPS 140-2) but *Can* accept risk that deviates from a Guideline (ex: NIST 800- series)

Example: Federal Cryptographic Standards

- **Deciding *Whether* to Encrypt:** The decision rests with the owner of the information to be protected based on a thorough risk analysis (evaluate the sensitivity of the information, identify the security controls needed)
- **Deciding *How* to Encrypt:** Defined in FIPS 140-2 Security Requirements for Cryptographic Modules; if the information owner determines that encryption should be used, such encryption must be validated according to FIPS 140-2 or by the National Security Agency (NSA)

Note: Use Of Unvalidated Cryptography

- FIPS 140-2 precludes the use of unvalidated cryptography for the cryptographic protection of sensitive or valuable data within Federal systems. Unvalidated cryptography is viewed by NIST as providing no protection to the information or data - in effect the data would be considered unprotected plaintext. If the agency specifies that the information or data be cryptographically protected, then FIPS 140-2 is applicable. In essence, if cryptography is required, then it must be validated.
- With the passage of the Federal Information Security Management Act (FISMA) of 2002, there is no longer a statutory provision to allow for agencies to waive mandatory Federal Information Processing Standards (FIPS). The waiver provision had been included in the Computer Security Act of 1987; however, FISMA supersedes that Act. Therefore, the references to the "waiver process" contained in many of the FIPS listed below are no longer operative.
- Reference: http://csrc.nist.gov/groups/STM/cmvp/index.html

DOE OCIO's Approach to Authorizations

- **Approach:** *Consider* all the Guidance and *Follow* all the mandatory Standards (ex: FIPS 140-2)
- **Benefits:**
  - Achieves security goals indicated by the controls (ex: SC-13)
  - Achieves FISMA compliance goals
  - Avoid need for mitigations that cost time and money
  - Avoid need for additional POA&Ms
  - Achieve system Authorizations faster
  - Reward vendors who have invested the effort, time and money to comply with Federal standards

Government Needs vs. Industry Needs

- **Government Needs:** Commercial solutions that are:
  - Cost-effective
  - Easy to Acquire
  - Easy to Secure
  - Easy to Assess & Authorize
  - Easy to Implement
- **Industry Needs:** Satisfied customers that continue to acquire commercial products and services

Conclusions

- When Government and Industry needs are all successfully met, a classic *"Win-win"* has occurred
- To those vendors that comply with the applicable government standards: "Thank you!"
- To those who do not: "What can you do to help your government customers?"

THANK YOU FOR YOUR TIME!

QUESTIONS?