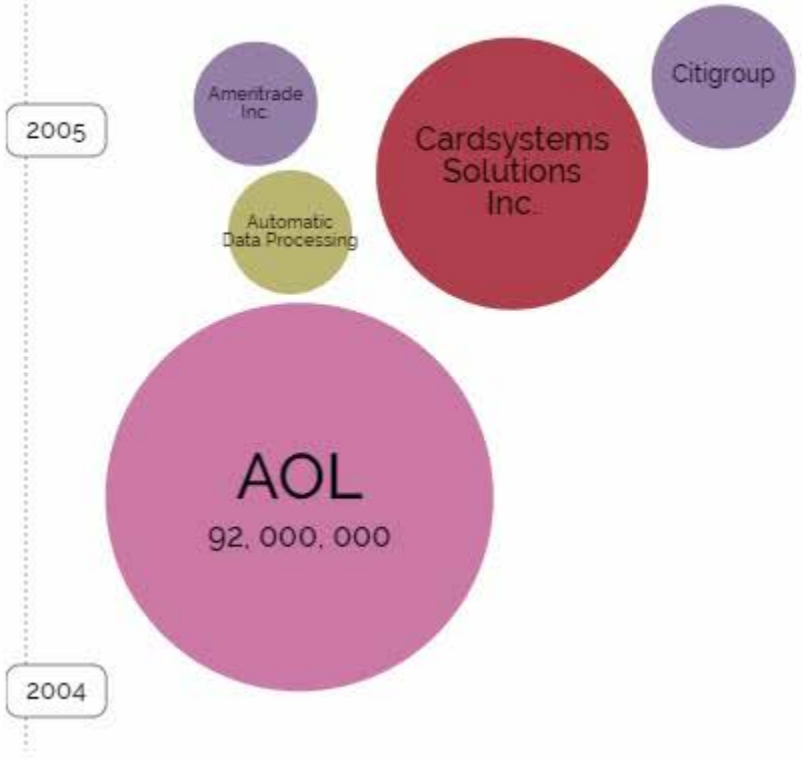
Federal Utility Partnership Working Group Seminar

FRCS CYBERSECURITY

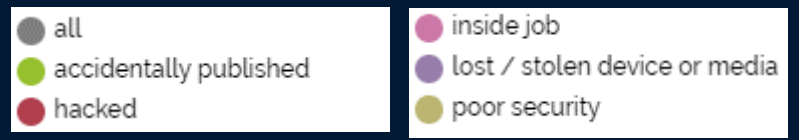
DEPSECDEF Cyber Memo Review

WHO'S **LURKING** ON **YOUR NETWORK?**

WORLD'S BIGGEST
DATA BREACHES (2004 – 2017)

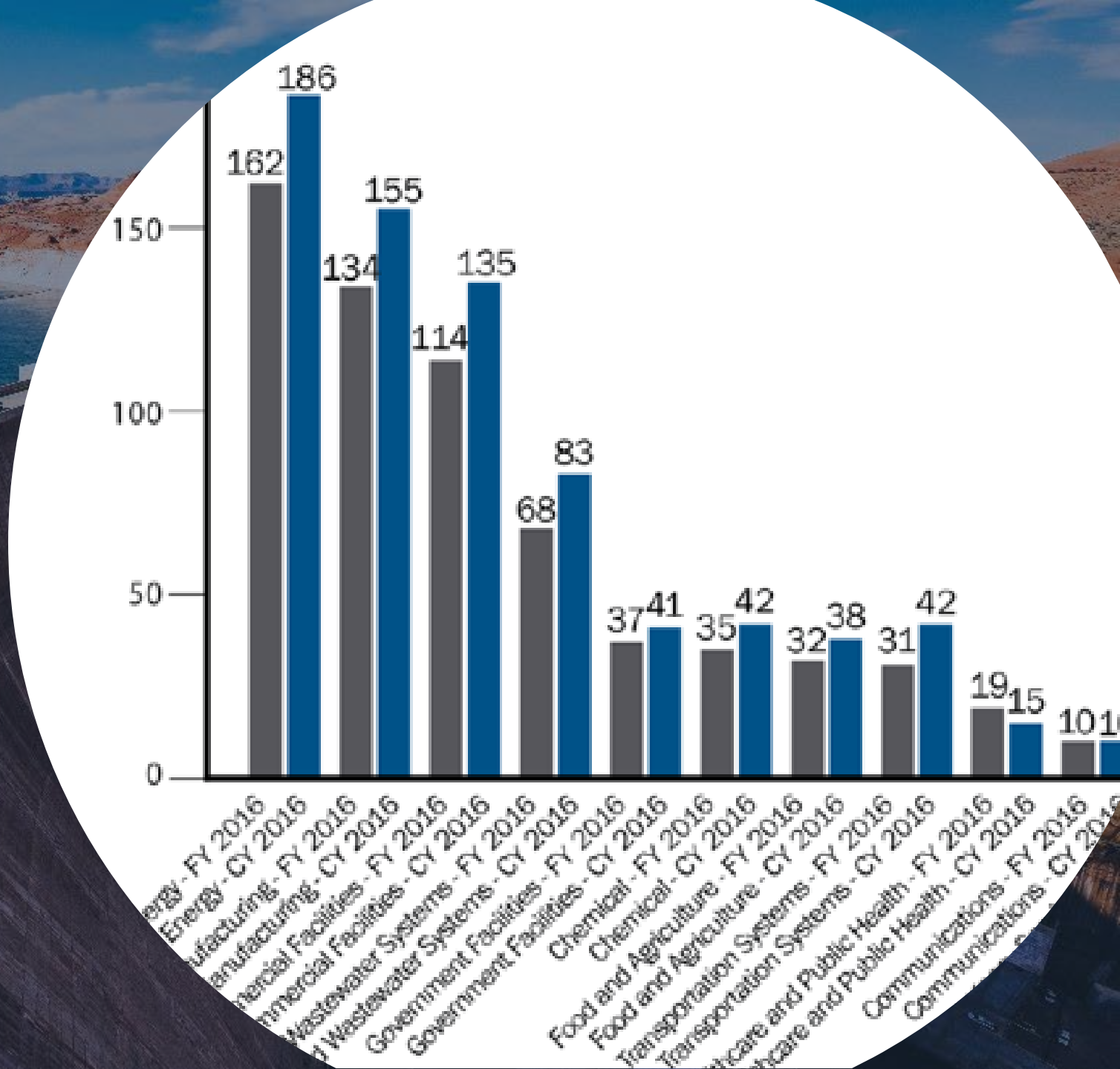


Year	2015	2016	2017
# of U.S. Breaches	780	1,093 (↑40%)	1,579 (↑44%)



Sources:
Information is Beautiful: World's Biggest Data Breaches and Identity Theft Resource Center (ITRC): 2017 Annual Data Breach Year-End Review.

According to ICS-CERT, the Energy Sector has the most vulnerabilities reported.



KEY FOCUS AREAS

1

STANDARDS & DRIVERS

Your network and devices may already be compromised

2

KNOW YOUR RESOURCES

In our connected world, weak links are vulnerabilities

3

IMPLEMENT HYGIENE

Small steps towards security can result in major improvements

4

SETUP YOUR PROGRAM

Know how to thwart risks and protect your organization

It is critical to be proactive and take the necessary measures to ensure the security of your devices and systems. Strong defense begins with **YOU.**

OT VULNERABILITIES DISRUPT MISSIONS

NOTIONAL MISSION THREAD CRITICAL PATH

An adversary could disrupt, degrade, or deny a mission by targeting the foundational assets that underpin the system of systems.

DOD CONTROL SYSTEMS

STRATEGY & POLICY MILESTONES

DEPSECDEF MEMO 19 JULY 2018

- 2018 National Defense Strategy articulates DoD' s intent to invest in cyber defense, resilience, and the continued integration of cyber capabilities into the full spectrum of military operations. Secure and resilient Control Systems (CS) are essential to providing warfighting capabilities, executing critical missions, and projecting power.
- To enhance cybersecurity risk management for CS, DoD must
  - **Implement standardized best practices**
  - **Improve CS information sharing**
  - **Advance cyber assessment capabilities**
  - **Maintain CS training, and**
  - **Establish a reporting requirement to ensure CS cybersecurity accountability.**

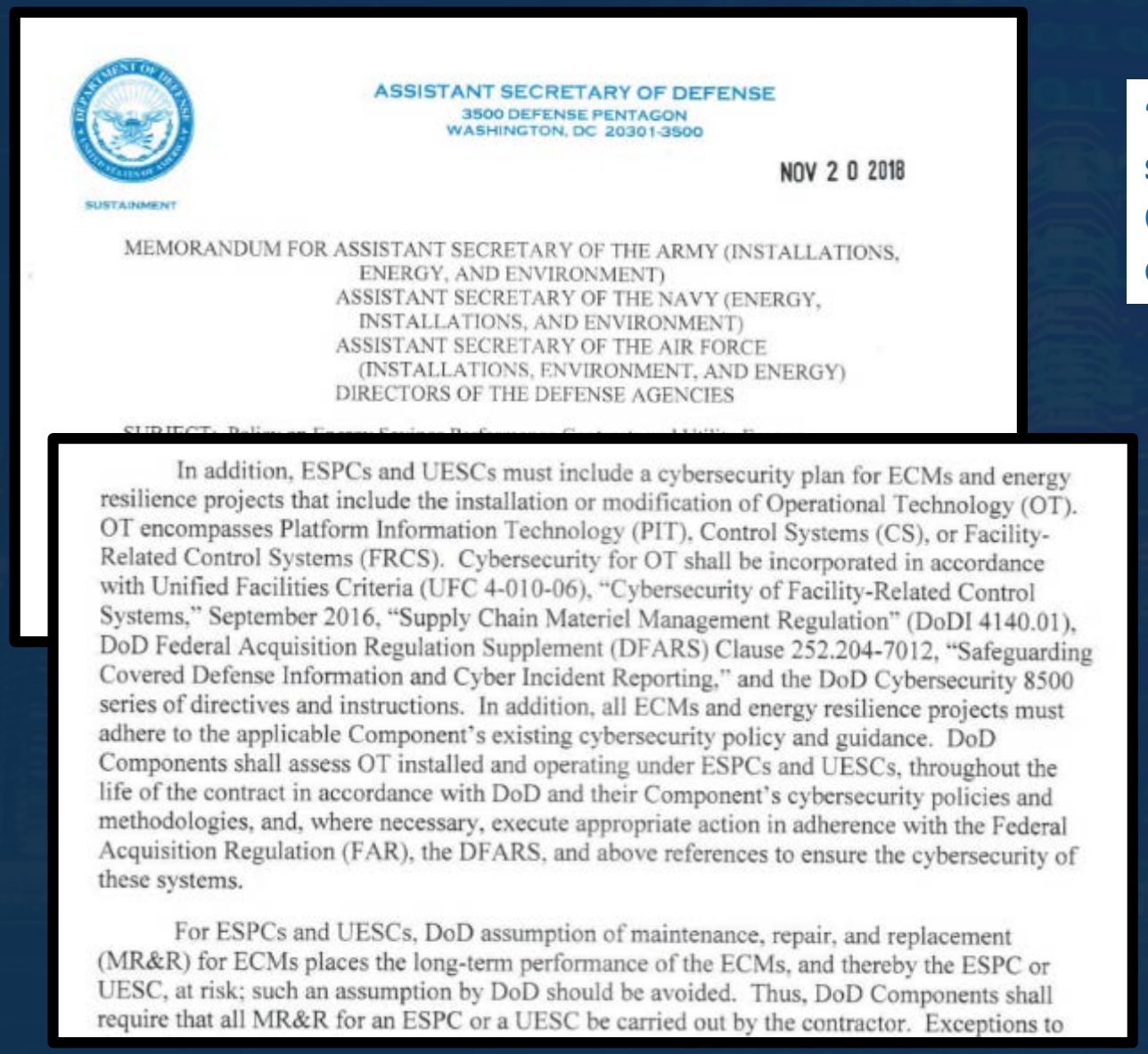
"CS consist of systems, devices, & networks designed to monitor or control specific processes (e.g. electricity & utility management, shipboard or aircraft mgmt systems, building automation, fuel distribution management, & chemical measurements)."

DEPSECDEF MEMO 19 JULY 2018 (CONT.)

DoD Components will be accountable for the following:

- **Best Practices and Tactics, Techniques, and Procedures:** Reduce operational risks posed by adversarial actions by implementing basic cybersecurity practices as well as proactively incorporating processes to harden CS infrastructure supporting Defense Critical Infrastructure (DCI).
- **Information Sharing:** Enhance overall situational awareness and threat, vulnerability, and mitigation analysis by increasing availability and access to data pertaining to CS risk management.
- **Scorecard and Assessments:** Illuminate risk management activities and incorporate criteria to assess CS cybersecurity practices to synchronize the Department's CS activities.
- **Training:** Baseline the Department's overall CS threat knowledge and risk management practices to increase the security posture of DCI.
- **Reporting:** Update status of CS cybersecurity efforts.

ASD MEMO FOR ESPC AND UESC



ASSISTANT SECRETARY OF DEFENSE
3500 DEFENSE PENTAGON
WASHINGTON, DC 20301-3500

SUSTAINMENT

NOV 2 0 2018

MEMORANDUM FOR ASSISTANT SECRETARY OF THE ARMY (INSTALLATIONS, ENERGY, AND ENVIRONMENT)
ASSISTANT SECRETARY OF THE NAVY (ENERGY, INSTALLATIONS, AND ENVIRONMENT)
ASSISTANT SECRETARY OF THE AIR FORCE (INSTALLATIONS, ENVIRONMENT, AND ENERGY)
DIRECTORS OF THE DEFENSE AGENCIES

In addition, ESPCs and UESCs must include a cybersecurity plan for ECMs and energy resilience projects that include the installation or modification of Operational Technology (OT). OT encompasses Platform Information Technology (PIT), Control Systems (CS), or Facility-Related Control Systems (FRCS). Cybersecurity for OT shall be incorporated in accordance with Unified Facilities Criteria (UFC 4-010-06), "Cybersecurity of Facility-Related Control Systems," September 2016, "Supply Chain Materiel Management Regulation" (DoDI 4140.01), DoD Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting," and the DoD Cybersecurity 8500 series of directives and instructions. In addition, all ECMs and energy resilience projects must adhere to the applicable Component's existing cybersecurity policy and guidance. DoD Components shall assess OT installed and operating under ESPCs and UESCs, throughout the life of the contract in accordance with DoD and their Component's cybersecurity policies and methodologies, and, where necessary, execute appropriate action in adherence with the Federal Acquisition Regulation (FAR), the DFARS, and above references to ensure the cybersecurity of these systems.

For ESPCs and UESCs, DoD assumption of maintenance, repair, and replacement (MR&R) for ECMs places the long-term performance of the ECMs, and thereby the ESPC or UESC, at risk; such an assumption by DoD should be avoided. Thus, DoD Components shall require that all MR&R for an ESPC or a UESC be carried out by the contractor. Exceptions to

"All data required to provide privatized utility services" be handled as Covered Defense Information/ Controlled Unclassified Data – new, renewing, and existing utility service contracts

FOR IMMEDIATE ACTION - Assistant Secretary of Defense for Sustainment (ASD(S)) Supplemental Guidance for the Utilities Privatization Program Memorandum Feb 7, 2019. DoD recognizes the risk posed by emerging threats to its mission critical cyber-supported Facility Related Control System (FRCS). FRCS cyber security enables resilience of essential utilities and other key services that support mission requirements. **Utility system owners are accountable for system operation resilience and cybersecurity, including the safeguarding of CDI related to utility services.**

PRIVATIZED UTILITIES MUST
CREATE CYBER PLANS

All Department energy / UP contracts must complete a Cyber Risk Management Plan (CRMP) containing the following:

- **System Security Plan (SSP)**
- **Plan of Action and Milestones (POA&M)**
- **Incident Response Plan & Procedures**
- **Data Handling & Marking Policy**

Valuable Data Must be Protected – Use NIST SP 800.171 as a guide.

CYBER RISK MANAGEMENT FOR

UTILITY SERVICE PROVIDERS

ASD(S) Supplemental Guidance for the Utilities Privatization Program Memorandum Feb 7, 2019 requires:

1) “All data required to provide privatized utility services” be handled as Covered Defense Information/Controlled Unclassified Data – new, renewing, and existing utility service contracts

DFARS 252.204-7012	**DFARS 252.227-7013**
Safeguarding Covered Defense Information and Cyber Incident Reporting	Rights in Technical Data - Non-commercial Items

2) Cyber Risk Management Plan (CRMP) for systems owned and operated by Utility Service Provider that process and store CDI/CUI

CRMPs IAW NIST SP 800-171 showing compliance with DFARS

UTILITY SERVICE PROVIDER
DECISION TREE

Privately Owned?

Yes

3rd Party System

No

DoD Mission Assurance Benchmarks IAW DTRA Assessment Guidelines

JMAA Benchmarks

CRMP

For Corporate IT business systems that host or transmit Controlled Unclassified Information (CUI)

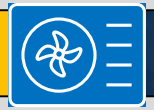
RMF Process

Supporting Implementation Resources Described in Depth on Following Slides

CRMP

- Event/Incident Communications Plan
- Security Assessment Report
- Event/Incident Response Plan
- System Security Plan
- Security Audit Plan
- Plan of Actions & Milestones
- Information Systems Contingency & CONOPS Plan
- US-CERT Incident Response Form
- CJCSM 6510.01

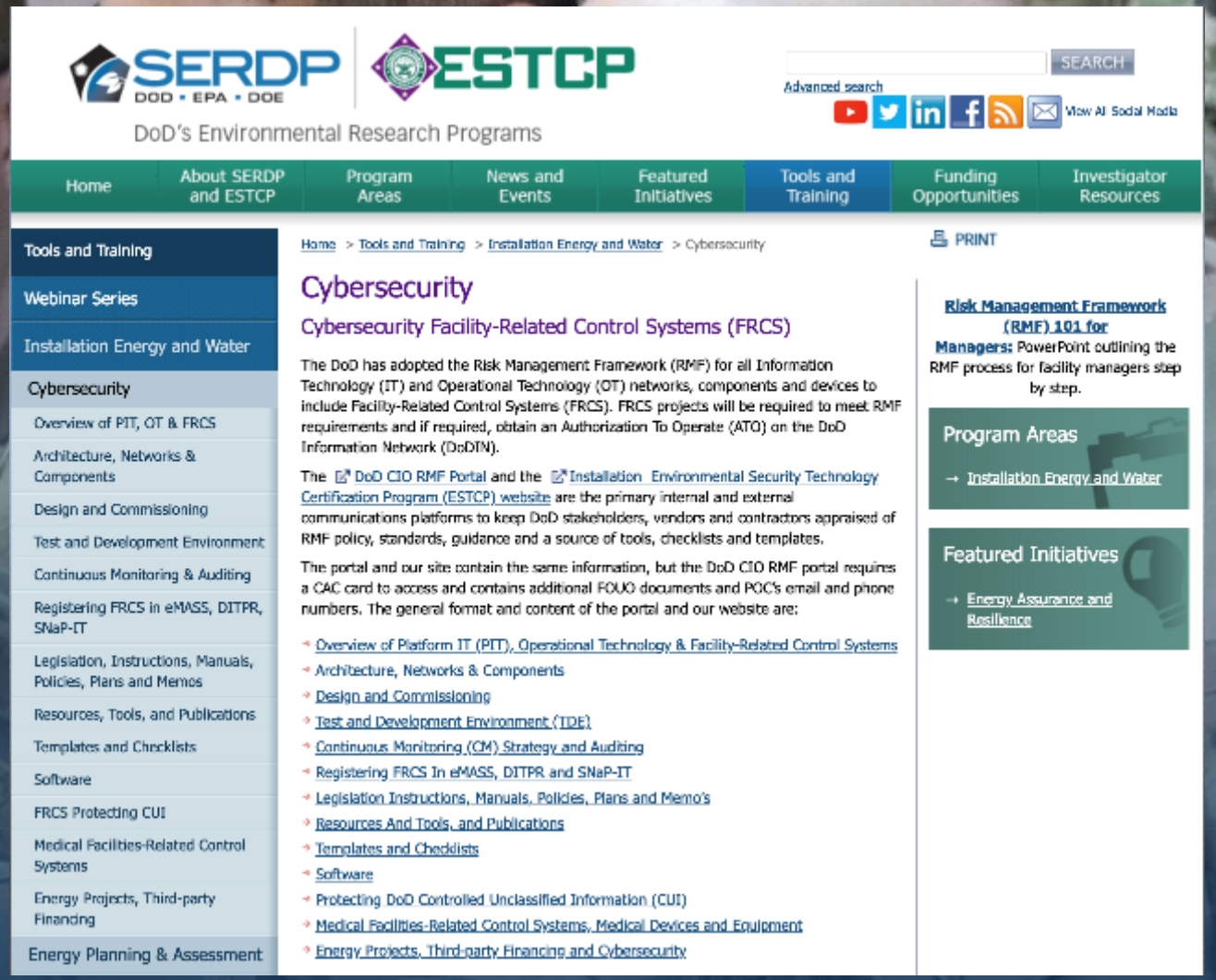
ESTCP Website



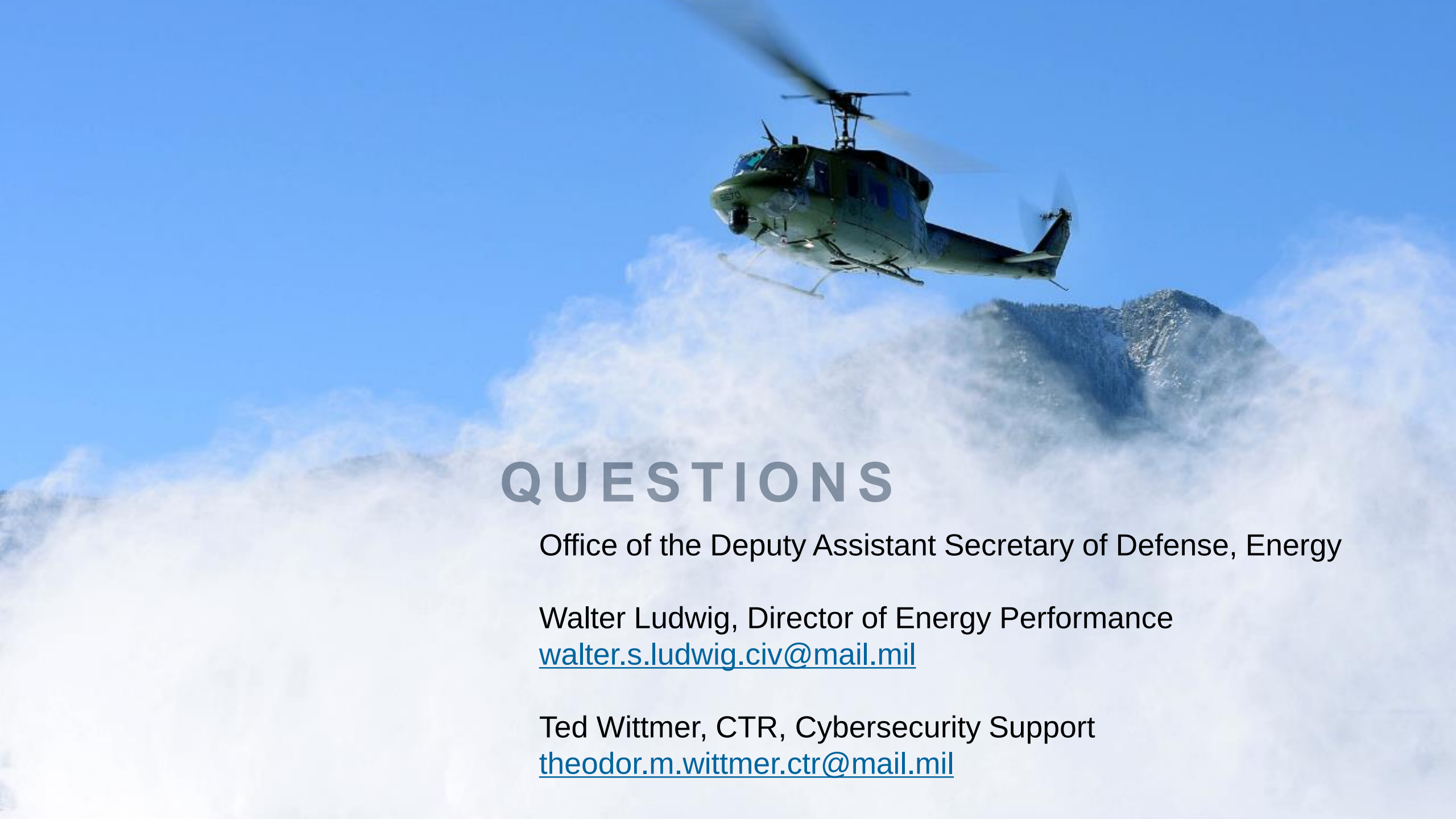
NIST 800-171

CSET Tool

DOD CS / OT CYBERSECURITY RESOURCES



https://serdp-estcp.org/Tools-and-Training/Installation-Energy-and-Water/Cybersecurity



QUESTIONS

Office of the Deputy Assistant Secretary of Defense, Energy

Walter Ludwig, Director of Energy Performance
walter.s.ludwig.civ@mail.mil

Ted Wittmer, CTR, Cybersecurity Support
theodor.m.wittmer.ctr@mail.mil