Waterpower Week

“Hear from the Federal Energy Regulatory Commission”
Thursday March 14th

FEDERAL ENERGY REGULATORY COMMISSION
Office of Energy Infrastructure Security (OEIS)

David Andrejcak
Deputy Office Director

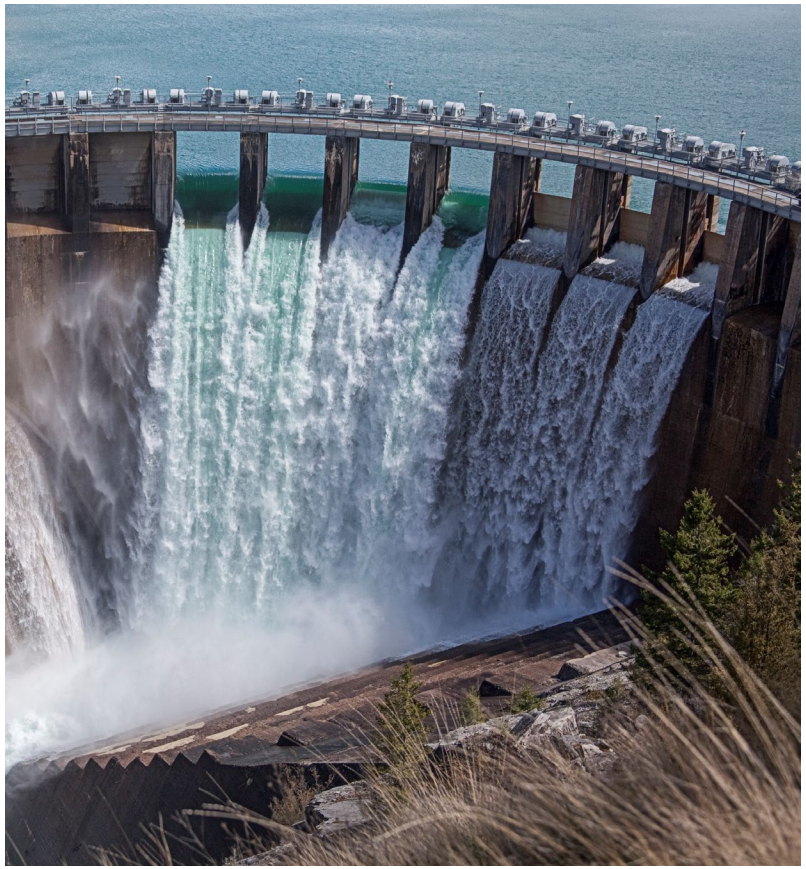
Disclaimer

The views expressed in this presentation are my own and do not necessarily represent
the views of any Commissioner or the Commission.

#whoami

David Andrejcak

- Deputy Office Director since 2014 for the Office of Energy Infrastructure Security at FERC
- Prior Management experience at Dominion
- BSEE from Penn State (a long time ago)
- Office Focus - Communicate and find comprehensive solutions to potential risks to FERC-jurisdictional facilities from cyber attacks and physical threats including electromagnetic pulses.
- Cybersecurity Best Practices and Industry Outreach



FERC Overview

FERC Two-Pronged Approach

Identify and Promote voluntary ***Best Practices*** to Address Advanced and Targeted Threats to Key Facilities

Establish Broad Foundational **Regulations**

“Regulations will define minimum expected cybersecurity practices or outcomes but the Administration encourages and will support further efforts by entities to exceed these requirements."

Critical Infrastructure Threats

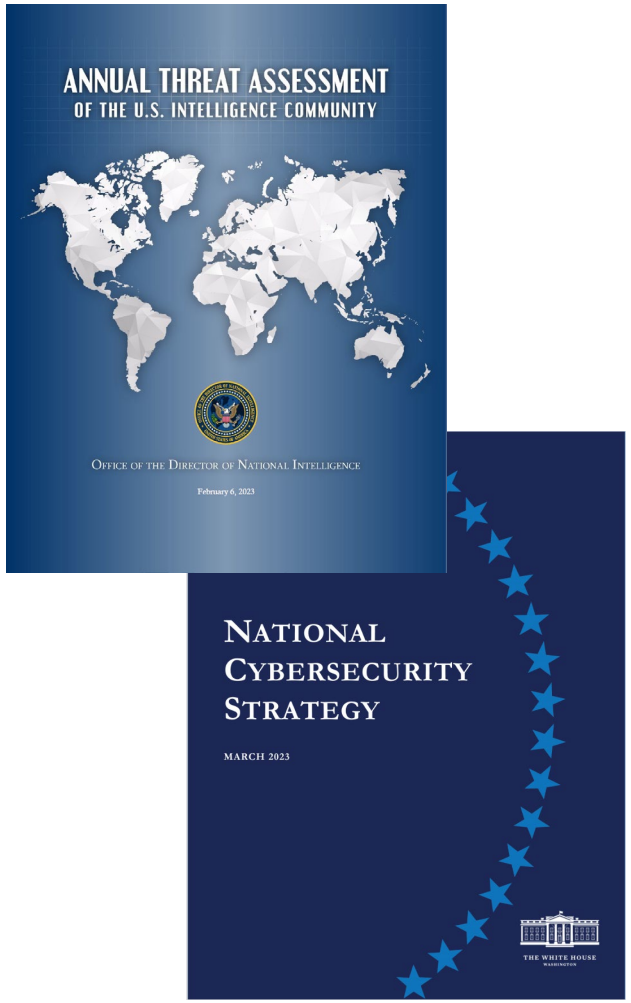
"China almost certainly is capable of launching cyber attacks that would disrupt [CI] services within the [US], including against oil and gas pipelines and rail systems."
[1 p.10]

On July 21, 2021, CISA issued a Cybersecurity Advisory entitled "Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013"[3]

"The [PRC] now presents the broadest, most active, and most persistent threat to both government and private sector networks…"
[2 p.3]

"Russia is particularly focused on improving its ability to target [CI], including underwater cables and [ICS], in the [US] and allied and partner countries…"
[1 p.15]

"Russia remains a persistent cyber threat as it refines its cyber espionage, attack, influence, and disinformation capabilities…"
[2 p.3]



"The governments of Iran and [North Korea] are similarly growing in their sophistication and willingness to conduct malicious activity in cyberspace."
[2 p.3]

"Iran's opportunistic approach to cyber attacks makes [CI] owners in the [US] susceptible to being targeted by Tehran, particularly when Tehran believes it must demonstrate that it can push back against the [US] in other domains."
[1 p.19]

"[North Korea] probably possesses the expertise to cause temporary, limited disruptions of some [CI] networks and disrupt business networks in the [US]."
[1 p.21]

https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf

Sources:
[1] ODNI: Annual Threat Assessment of the U.S. Intelligence Community
[2] Whitehouse: National Cybersecurity Strategy 2023
[3] CISA: Alert AA21-201A

Cyber Architecture Assessment Overview

- ❑Overview
- ❑Pre-Assessment Virtual Meeting
- ❑Day 1 & 2 (covered next slide)

PURPOSE OEIS provides voluntary, in-depth assessments of a utility's Information Technology (IT) and Operational Technology (OT) systems and networks.

GOAL The voluntary assessments provide entities with a comprehensive understanding of their current cybersecurity posture benchmarked against best practices from industry and the federal government.

RESOURCE COMMITMENT A two-day assessment requires subject matter experts from across the organization: IT Management, Active Directory, Cloud Management, Database and Application Management, Network Operations, Edge Protection, Security Operations, and OT Engineers. The opening and closing discussions should be attended by the C-Suite.

High Impact Vectors

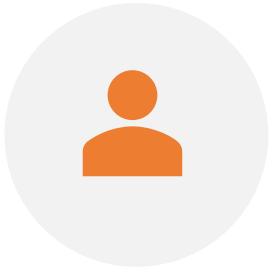
Exploitation of known vulnerabilities

Phishing

Passwords exposed through breach and reuse

Use of legitimate remote management software

Technology Focus



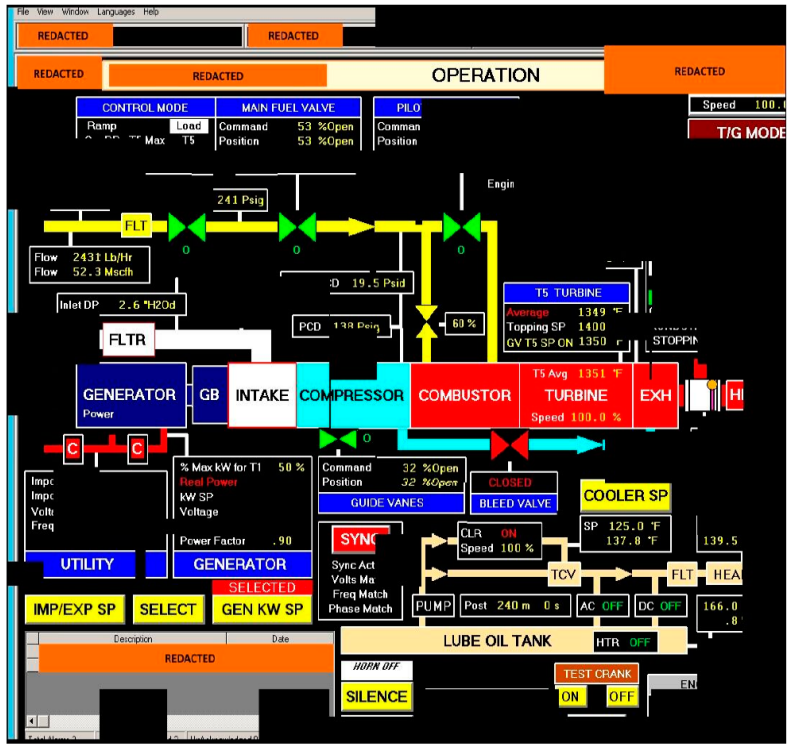
ACTIVE DIRECTORY

REMOVABLE MEDIA

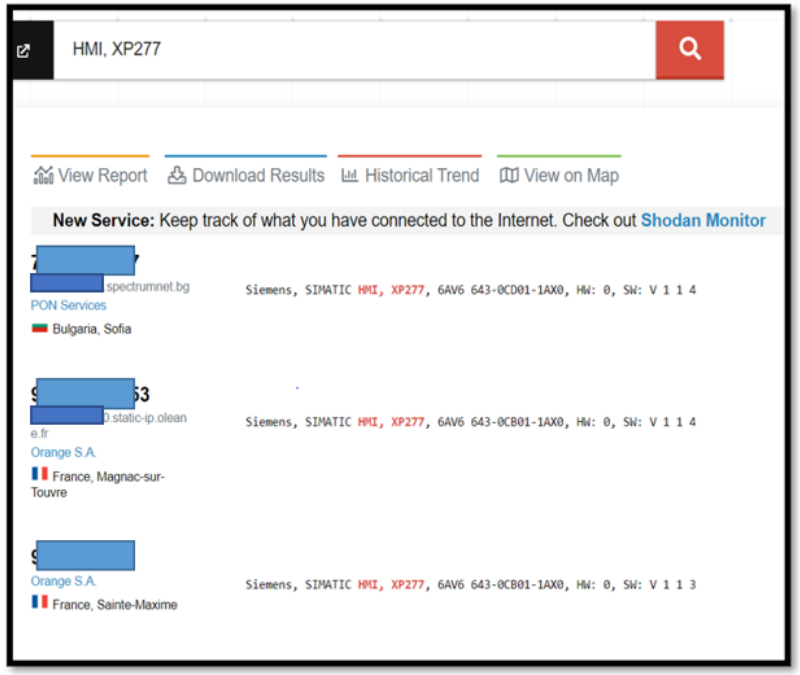
BACKUPS

OPEN-SOURCE SOFTWARE

Open-Source Information



Source: https://us-cert.cisa.gov/ncas/alerts/TA18-074A



Source: Shodan

Best Cybersecurity Practices

- Phishing Prevention Training
- Jump Host Hardening
- Identity and Access Management
- Recurring Background Investigations
- Firewall Deny Log Review
- Incident Response Playbooks
- Procurement / Supply Chain
- Continuity of Operations
- Penetration Testing

Contact Information

David.Andrejcak@ferc.gov