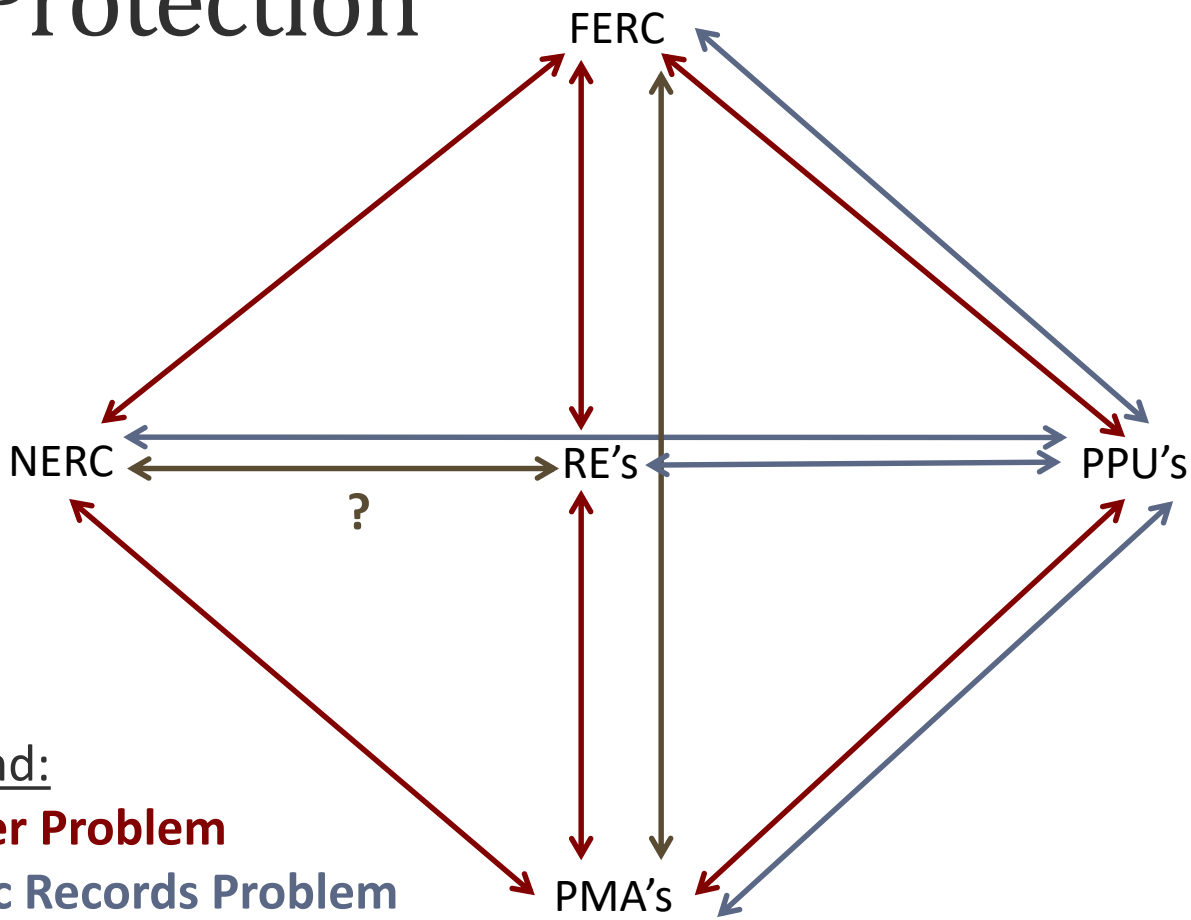
Critical Infrastructure Information: Threat of Disclosure Under Open Records Requirements & FOIA Requests - Federal Legislation and Regulation; Arizona Response

APPA Legal Seminar
October 21, 2013

Robert S. Lynch
Robert S. Lynch & Associates, Phoenix, Arizona
rsylnch@rslynchaty.com

Communication Paths & Information Locations Needing CEII Protection



Color Legend:

FOIA Waiver Problem

State Public Records Problem

FOIA Protection

Existing Federal Legislation and Regulations

- 6 USC § 133 - Protection of voluntarily shared critical infrastructure information
- 42 USC § 5195c - Critical infrastructure protection
- 18 CFR 388.113 - Accessing critical energy infrastructure information

Pending Federal Legislation: H.R. 624

- Title: Cyber Intelligence Sharing and Protection Act (CISPA)
- Purpose: To provide for the sharing of certain cyber threat intelligence and cyber threat information between the intelligence community and cyber security entities, and for other purposes.
- CIP Language: Pages 16-19
- Timeline:
  - 2/13/2013 Introduced in House.
  - 4/15/2013 Reported (Amended) by the Committee on Intelligence. H. Rept. 113-39.
  - 4/18/2013 Passed/agreed to in House: On passage Passed by the Yeas and Nays: 288 - 127 (Roll no. 117).
  - 4/22/2013 Received in the Senate and Read twice and referred to the Select Committee on Intelligence.

Pending Federal Legislation: H.R. 624 (cont'd)

Language Description from House Intelligence Committee Press Release:

- Strong Protections for Privacy and Civil Liberties: The bill has very narrow definitions that permit only the voluntary sharing by the private sector of a very limited category of information—cyber threat information—and permits only the sharing of such information for cybersecurity purposes, a similarly limited term.
  - The bill protects privacy by prohibiting the government from forcing private sector entities to provide information to the government, by mandating the government to "anonymize" or "minimize" any information it receives from the government, and by explicitly authorizing and encouraging the government to create procedures to protect privacy. It also strictly limits the private-to-private sharing to only cyber threat information to ensure no information can be used for other non-cyber purposes.

Critical Infrastructure Protection

- CIP 3
  - Title: Cyber Security —Security Management Controls
  - Number: CIP-003-5
  - Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.
- CIP 4
  - Title: Cyber Security —Personnel & Training
  - Number: CIP-004-5
  - Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the BES from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.
- CIP 5
  - Title: Cyber Security —Electronic Security Perimeter(s)
  - Number: CIP-005-5
  - Purpose: To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

Executive Branch Action: Executive Order

- "Improving Critical Infrastructure Cybersecurity" Executive Order 13636 of February 12, 2013
- Policy (Sec. 1) – Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties. We can achieve these goals through a partnership with the owners and operators of critical infrastructure to improve cyber security information sharing and collaboratively develop and implement risk-based standards.

Executive Branch Action: Presidential Policy Directive

- Title: Presidential Policy Directive/PPD-21
- Subject: Critical Infrastructure Security and Resilience
- Purpose: The Presidential Policy Directive on Critical Infrastructure Security and Resilience advances a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure.
- Date: February 12, 2013

Current Arizona Legislation: A.R.S. § 39-126

A.R.S. § 39-126 – Federal Risk Assessments of Infrastructure; Confidentiality

Nothing in this chapter requires the disclosure of a risk assessment that is performed by or on behalf of a federal agency to evaluate critical energy, water or telecommunications infrastructure to determine its vulnerability to sabotage or attack.

New Arizona Legislation: S.B. 1324

- Title: Critical Infrastructure; Information Disclosure
- Purpose: All critical infrastructure and key resources information protected by federal law and provided to or in the possession of any state agency or political subdivisions is exempt from public disclosure and public records laws. The definition of "critical infrastructure information" is expanded to include emergency response plans and certain information related to a computer based or natural disaster.
- Timeline:
  - 1/31/2013 Introduced in Arizona State Senate
  - 2/25/2013 Passed by Arizona State Senate (Vote: 28—0); Introduced in Arizona State House of Representatives
  - 3/26/2013 Passed Arizona State House of Representatives (Vote: 58 – 2)
  - 4/5/2013 Signed by Arizona State Governor
  - 9/13/2013 Became Arizona State Law – Laws 2013, Chapter 69

Proposed Arizona Legislation: H.B. 2577

- Title: Public Records Exemption; Critical Infrastructure
- Purpose: “Critical energy infrastructure information” or “critical infrastructure” information that is possessed by the state or a local government is exempt from inspection, copying or other disclosure requirements of any state or local law or rule.
- Timeline:
  - 2/11/2013 Introduced to Arizona State House of Representatives, assigned to 2 committees
  - Final Disposition: Held in Committees

For More Information

- H.R. 624: Library of Congress
  http://thomas.loc.gov/cgi-bin/thomas
- CIP 3 thru 5: North American Reliability Corporation (NERC)
  http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
- Executive Order 13636
  http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
- Presidential Policy Directive 21
  http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil
- A.R.S. § 39-126: Arizona State Legislature
  http://www.azleg.gov/DocumentsForBill.asp?Bill_Number=SB1167&Session_ID=76
- S. B. 1324: Arizona State Legislature
  http://www.azleg.gov/DocumentsForBill.asp?Bill_Number=SB1324&Session_ID=110
- H.B. 2577: Arizona State Legislature
  http://www.azleg.gov/DocumentsForBill.asp?Bill_Number=HB2577&Session_ID=110