TCIPG

ANNUAL INDUSTRY WORKSHOP
NOVEMBER 6-7, 2013

INFORMATION SHARING IN THE ELECTRICITY SUB-SECTOR

SEPTEMBER 20, 2013

SCOTT R. MIX, CISSP

CIP TECHNICAL MANAGER, NERC

FUNDING SUPPORT PROVIDED BY DOE-OE AND DHS S&T

- The views and opinions expressed in this presentation are those of the presenter, and do not represent those of the North American Electric Reliability Corporation

EXECUTIVE ORDER (EO) 13636 AND PRESIDENTIAL POLICY DIRECTIVE (PPD) - 21

- In February 2013, the President announced two new policies:
  - EO 13636: Improving Critical Infrastructure Cybersecurity
    - Develop a technology-neutral cybersecurity framework
    - Promote and develop incentives for the adoption of cybersecurity practices
    - Enhance cybersecurity information sharing
    - Strengthen privacy and civil liberties protections

EO 13636 AND PPD-21

- PPD-21: Critical Infrastructure Security and Resilience
  - Develop a near real-time situational awareness capability
  - Evaluate and mature the public-private partnership
  - Update the National Infrastructure Protection Plan (NIPP)
  - Develop a comprehensive research and development plan

EO 13636 AND PPD-21

- NERC and industry experts represent the Electricity Sub-sector on all implementation working groups:
  - Stakeholder Engagement
  - Cyber-Dependent Infrastructure Identification (CDII)
  - Planning and Evaluation
  - Situational Awareness and Information Exchange (SAIE)
  - Incentives
  - Framework Collaboration
  - Assessments: Privacy and Civil Rights and Civil Liberties
  - Research and Development (R&D)

EO 13636 AND PPD-21 WORKING GROUPS

- **Cybersecurity Framework Development**
  - Work with the National Institute of Standards and Technology (NIST) to develop a voluntary, repeatable cybersecurity framework consisting of industry standards, guidelines, and best practices to promote the protection of critical infrastructure
    - Industry contribution via Requests for Information (RFI), workshops, and working group meetings
    - Status: Final draft was released on October 22; NIST will open a 45-day public comment period on the Preliminary Framework and plans to release the official framework in February 2014

EO 13636 AND PPD – 21 WORKING GROUPS

- **CDII**
  - Collaborate with industry and the Department of Energy to identify critical infrastructure where a cyber incident could result in catastrophic effects
    - Status: The Department of Homeland Security (DHS) will notify selected entities in fall 2013 that they have cyber dependent infrastructure and provide procedures for appeals from such designation

EO 13636 AND PPD – 21 WORKING GROUPS

- **Planning and Evaluation**
  - Update the NIPP to coordinate public-private efforts to improve infrastructure security and resiliency
    - Address international cooperation and interdependencies, develop policies for coordination, and address global issues such as foreign investment and supply chains
    - Industry contribution via RFIs, writing sessions, and draft comments
    - Status: Final draft was released on October 22; final document will go to the White House on November 8

EO 13636 AND PPD – 21 WORKING GROUPS

- **Incentives**
  - Direct the study of incentives for participating in the voluntary critical infrastructure cybersecurity program
    - Status: In June 2013, the Department of Treasury, the Department of Commerce, and DHS issued a report that recommended the Administration analyze six incentive categories to encourage industry participation in the cybersecurity program
    - DHS and Sector-Specific Agencies will socialize incentive recommendations with the revised NIPP and Cybersecurity Framework

EO 13636 AND PPD-21 WORKING GROUPS

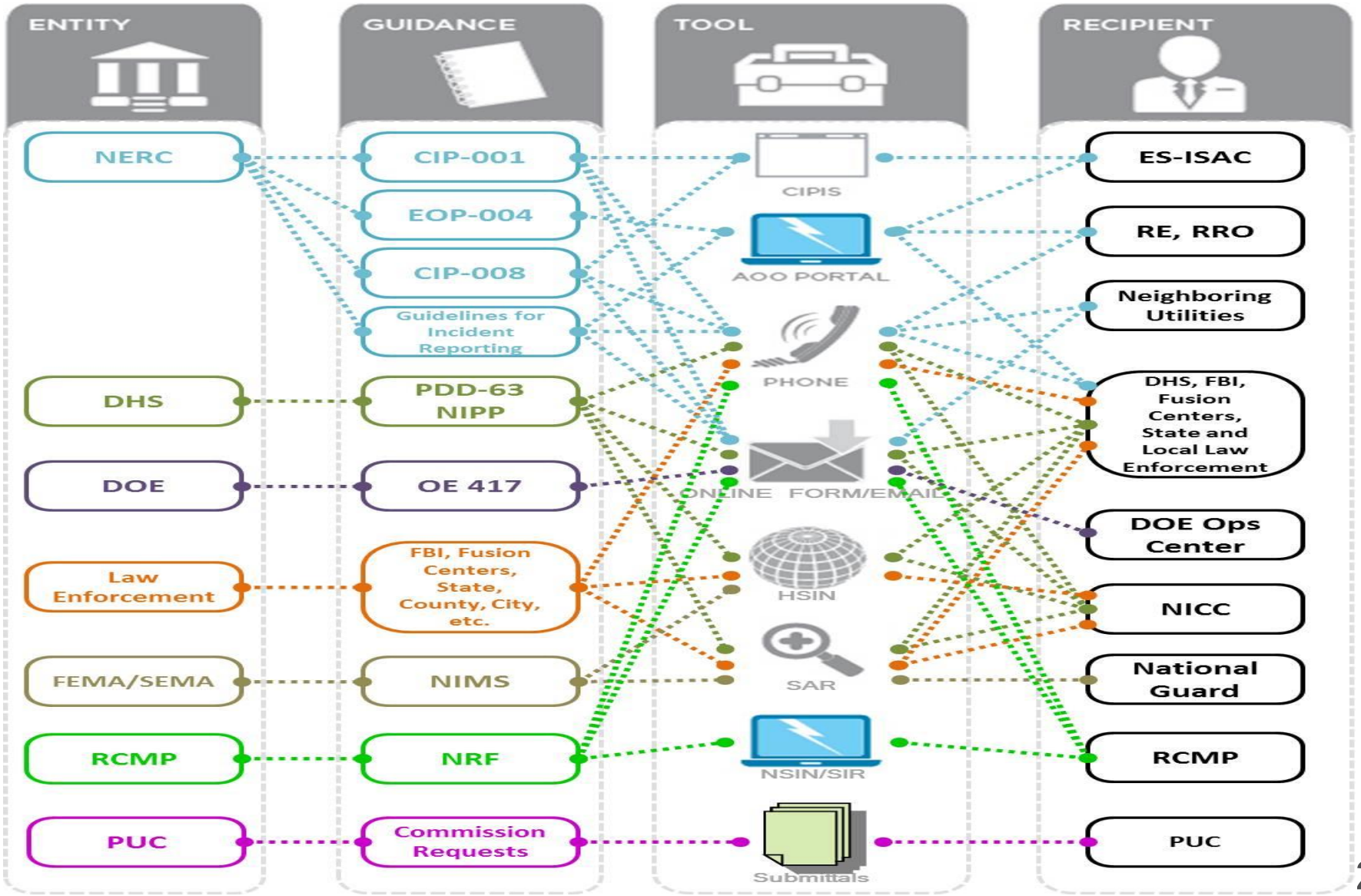
The remaining working groups continue to meet, but are less active at this time:

- SAIE is tasked with identifying functional relationships across the Federal Government and developing a situational awareness capability for critical infrastructure
- R&D is tasked with developing a critical infrastructure security and resilience R&D plan
  - Revised NIPP and the Cybersecurity Framework will contribute to this plan
  - Initial plan will be released in early 2014
- Assessments: Privacy and Civil Rights and Civil Liberties coordinates with representatives from across the interagency to assess civil rights and civil liberties impacts (government only)
- Stakeholder Engagement coordinates outreach to stakeholders throughout the implementation process
- Voluntary Programs supports the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and any other interested entities

IMPROVING INFORMATION SHARING

- NERC Critical Infrastructure Protection Committee (CIPC) Electricity Sector Information Sharing Task Force (ESISTF) report
  - Approved by NERC CIPC June 11, 2013
  - Endorsed by Electricity Sub-sector Coordinating Council July 11, 2013
  - Accepted by NERC Board of Trustees August 15, 2013
  - http://www.nerc.com/comm/CIPC/Electricity%20Sector%20Information%20Sharing%20Task%20For1/Electricity%20Sector%20Information%20Sharing%20Task%20Force%20Report.pdf

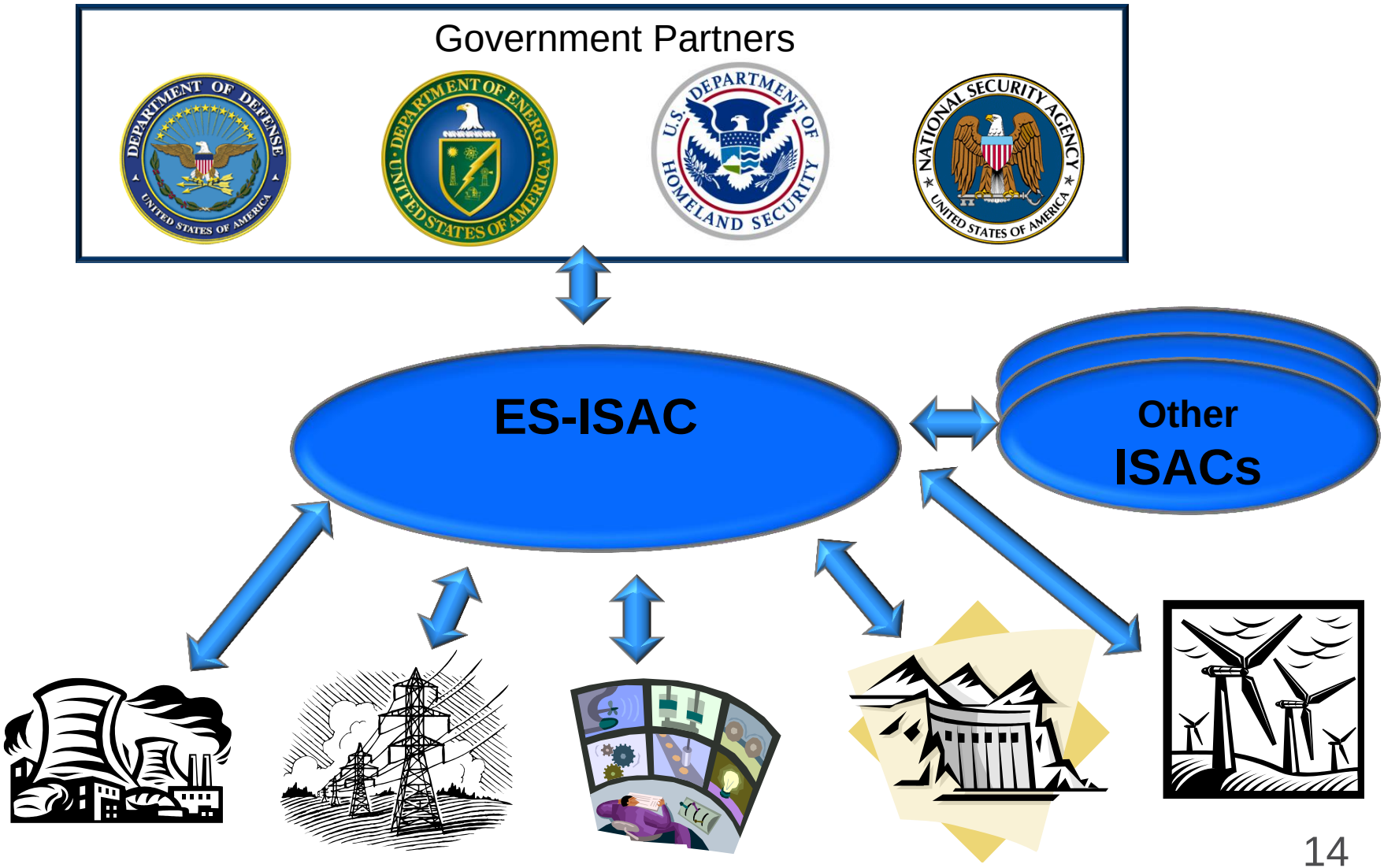
INFORMATION SHARING REPORT: PATHS



INFORMATION SHARING REPORT: RECOMMENDATIONS

1. Cultivate a trusting information-sharing environment
2. Promote recognition of the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) role as the Electricity Sub-sector's central hub for physical and cyber threat information sharing
3. Reduce complexity and redundancy of the reporting system
4. Implement technology to encourage unattributed information sharing
5. Improve information aggregation and collaborative analysis at the ES-ISAC

ES-ISAC ACTIVITIES: COLLABORATION AND COORDINATION



ES-ISAC ACTIVITIES: THE PORTAL

IOC Notice Reports, Watchlist Entries, Aggregated Lists, Blacklists

AOO Newsfeed, Weekly Updates, Webinar Notes, NERC Alerts (repost)

Anonymously share security incident information, generates report for your use, VERIS framework (beta)

File download links for auto-informing your security controls with regular updates

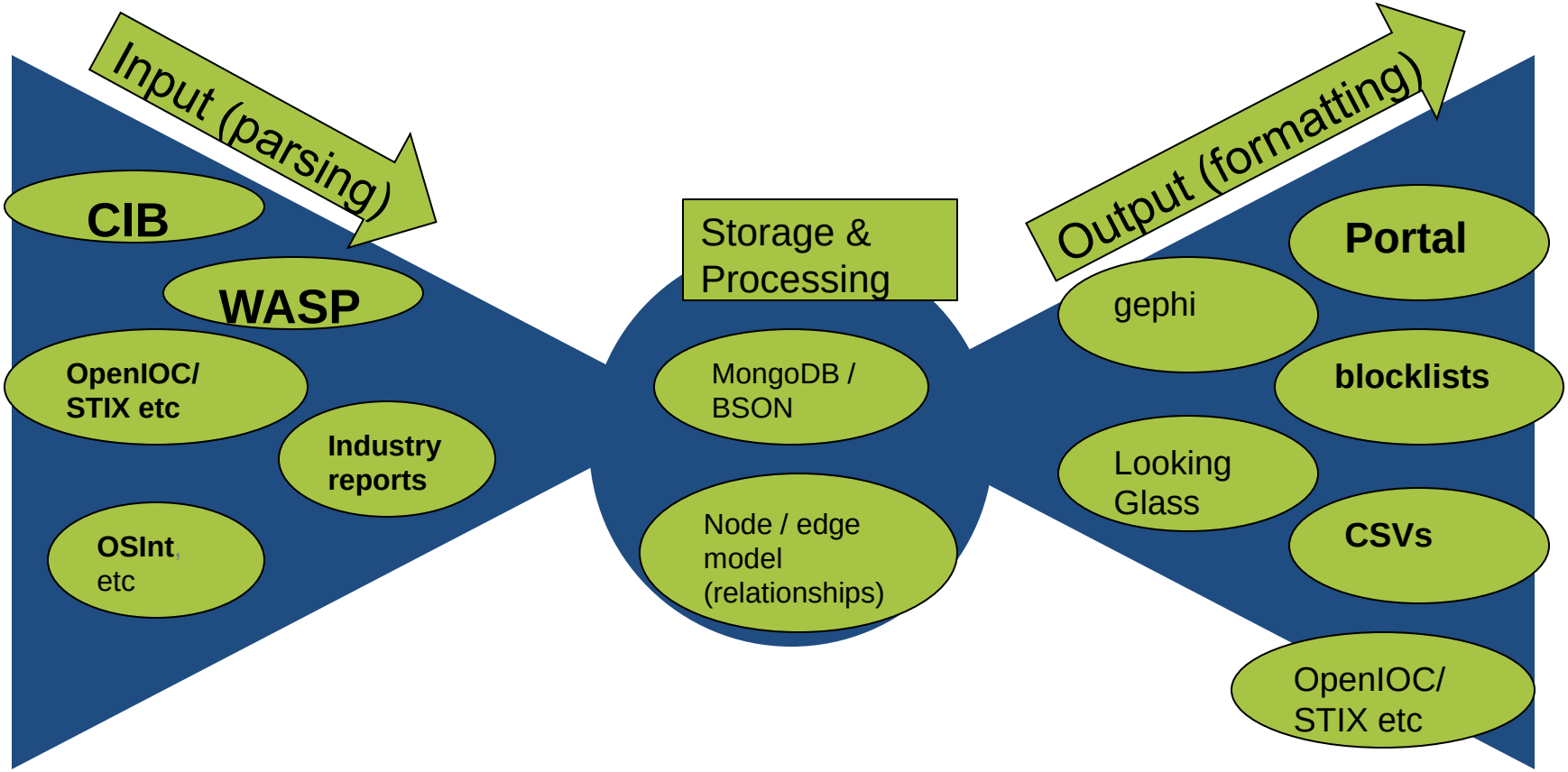
Auto-notice updates via Email

ES-ISAC ACTIVITIES: INDEX AND AOO

Wider audience, including US and Canadian Government agencies, regions, etc	Limited to Asset Owner & ES-ISAC Staff
"Read Only"	"Read/Write"
Actionable Information	News-worthy Information

Explicit Information Handling Expectations

ES-ISAC ACTIVITIES: BACK END WORKFLOW



ES-ISAC ACTIVITIES: CONTACT INFORMATION

ES-ISAC Portal

Are your security points of contact signed up?

Asset Owners and Operators personnel may register a portal user account by visiting
https://www.esisac.com/register.aspx

Please share malicious activity information **via EST** (beta) on the portal and further advising via
esisac@nerc.com

Orlando Stevenson, ES-ISAC Cyber Security Specialist- Critical Infrastructure
Office: 202-644-8077, Mobile: 202-360-2365
Orlando.Stevenson@nerc.net

QUESTIONS

SCOTT R MIX, CISSP
CIP TECHNICAL MANAGER, NERC
SCOTT.MIX@NERC.NET
215-853-8204

FUNDING SUPPORT PROVIDED BY DOE-OE AND DHS S&T