Industry role moving forward…

Discussion with National Research Council, Workshop on the Resiliency of the Electric Power Delivery System in Response to Terrorism and Natural Disasters

February 27-28, 2013

Who are we, and who is the industry?

- NERC
- NERC ES-ISAC
- Scale and complexion of the industry as a whole
- Industry character combines with critical sector interdependency to offer key insights on improved response

How NERC fits…

NERC MISSION

- To ensure the reliability of the bulk power system

INDUSTRY STRUCTURE, A RESPONSE VIEW…

- Generation
- Transmission
- Distribution
- Control

Industry Basics

- Large utilities, medium, small, muni, co-op
- Registered and unregistered entities
- 4 Interconnects, 16 Reliability Coordinators, 80 Balancing Authorities
- Mandatory and enforceable standards, including critical infrastructure protection
- Distributed risk and redundancy by nature-no Tier 1 out there
- SCADA/ICS cyber vulnerabilities lumped in two broad categories: bit flip, knowledge based
- Lots of all hazards experience with superior reliability performance and resilience experience

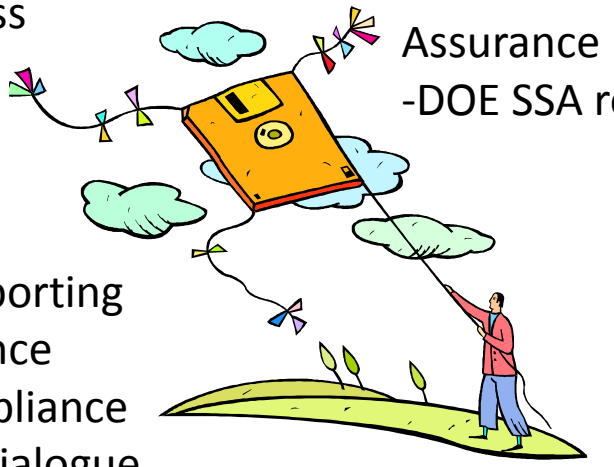
NERC ES-ISAC

- Information Sharing and Analysis Center
- Government recognized nexus for IS&A under National Infrastructure Protection Plan
- Positioned to deliver sector coordination support, threat fusion sharing, analysis for bulk power system rapid mitigation development and delivery
- Offers cyber and physical security expertise
- ARE NOT operators, WE ARE ***operationally informed***
- Maintain near real time grid common operational picture, wall of knowledge, wide area awareness, triage risk assessment and mitigation development/delivery
- Work closely with DHS, DOE (SSA), DoD, ESCC and other public and private sector collaborative partners
- HYDRA network to technology vendor supply chain, R&D labs and other SME community participants

Our World

Government Fusion
-DHS Critical Infrastructure
-DoD Mission Assurance
-DOE SSA relationship

BPSA wide area operational awareness
-ESF 12 Coordination
-Entity Relationships



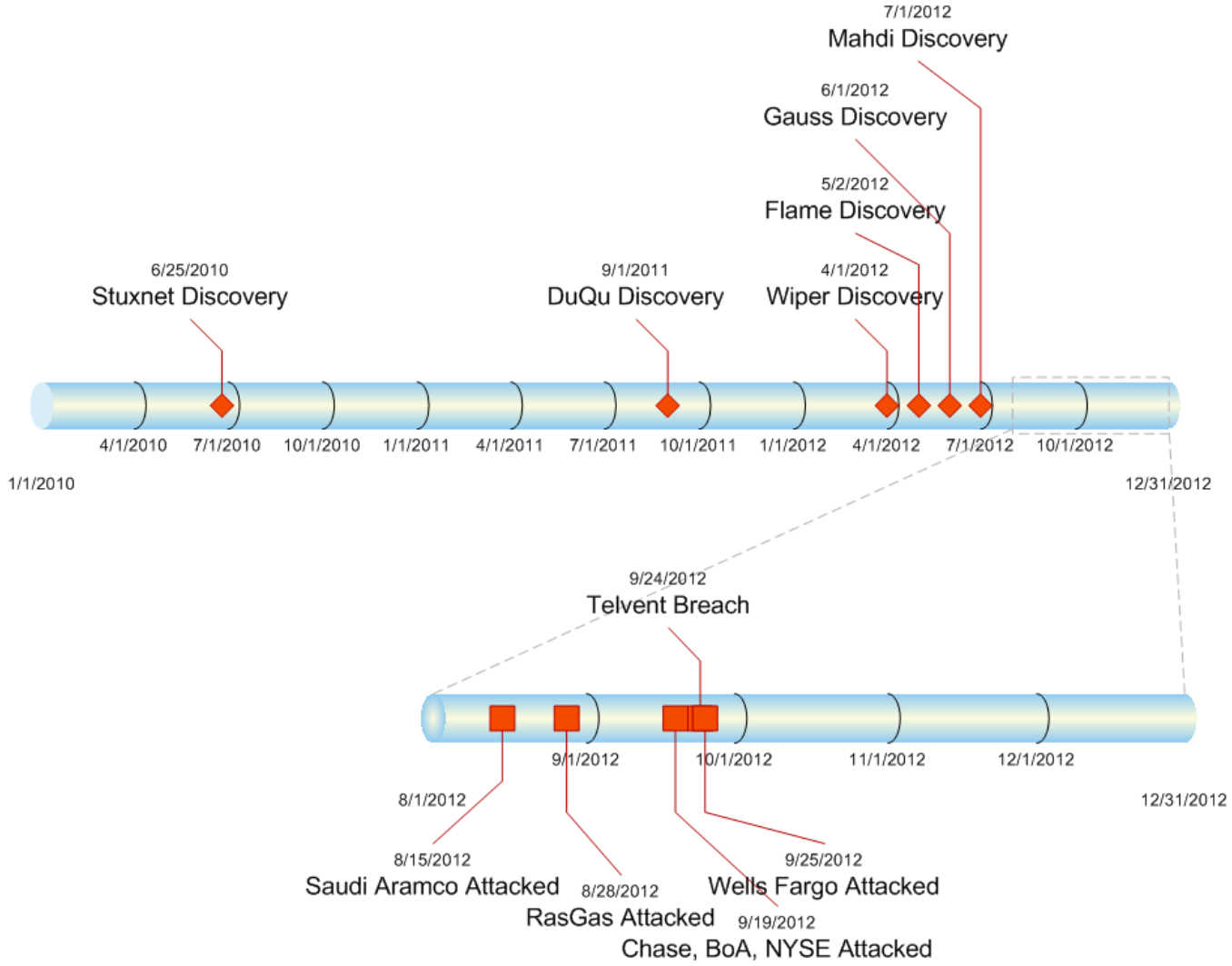
Entity Reporting
-Compliance
-Noncompliance security dialogue

ES-ISAC
-NIPP/UCG/ESCC Sector Coordination
-Cyber expertise

NERC Role Definition

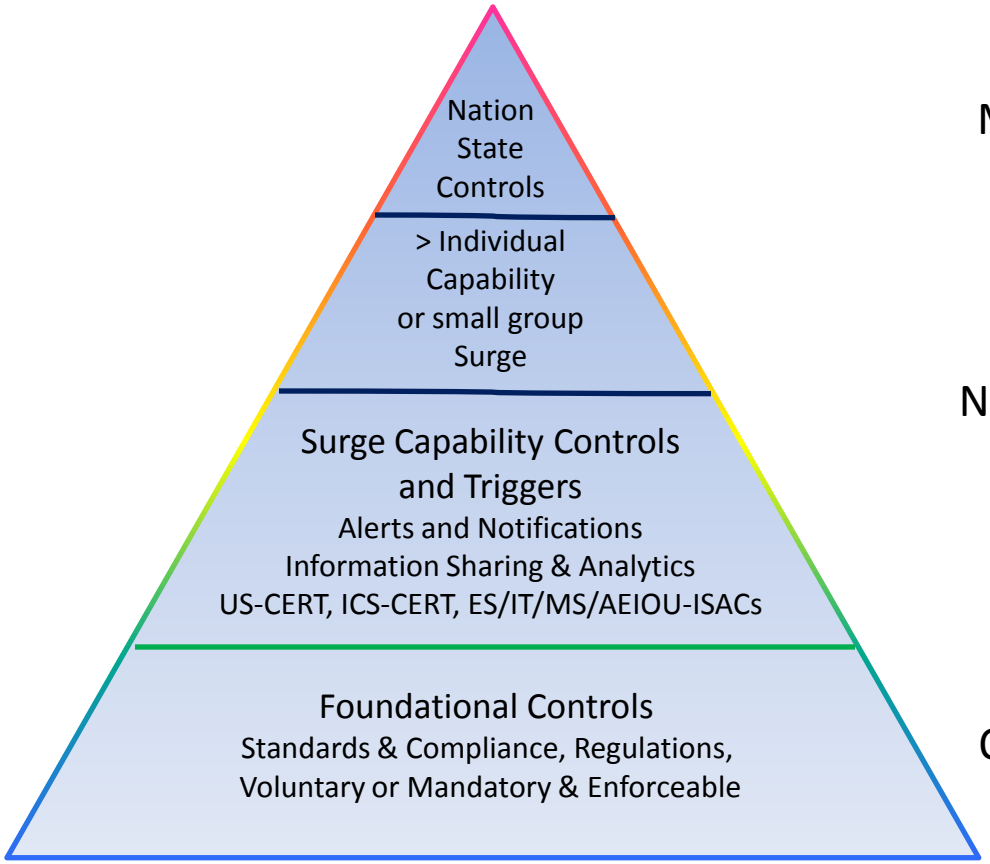
Internal Team	Role Definition
BPSA	-Operationally informed wide area awareness -Manage ESF-12 -Manage entity relationships
ES-ISAC	-NIPP approved ISAC nexus -UCG representation, ESCC support -Sector Coordination -Applied cyber expertise

Threat Landscape Overview



- More attacks occurring at a rapid pace.
- Growing in sophistication.
- Target: key sectors such as Financial Services and Oil and Natural Gas.

Strategy to Address Threats



National/Multi National

Advanced Threat Actors

Newly Discovered Vulnerabilities and Consequences

Vulnerability Consequences

Threats, Vulnerabilities and Consequences

Multi-National Policies

National Policies

Local and Organizational Policies

Remembering the Essentials of Optimal Response

- Lifecycle considerations left and right of boom
- Superlative sector level coordination
- Operator technical prowess, extemporaneous adaptability
- SME insight precisely and rapidly applied
- Fog of war avoidance
- Levering resilience multipliers
- Successful recovery positioning

What really gets us there…

- Active and coordinated participant engagement
- Durable communication of actionable knowledge
- Availability of wide area awareness, triage risk and analytic understanding
- Taking complexity and pre-event “do-ables” off the table
- Effective mutual aid governance
- Deer in headlights avoidance: applying imagination, training, exercise and learning pre-event
- Layers of defense, multipliers of resilience
- Resilience aware systems design, standards development, process architectures, cyber hygiene and compliance discipline
- Assuring response structures are sustainable

Reasons industry is central to response improvement…

- Regional challenges drive innovation
- Owner-operator perspective is where operator SME talent resides
- It’s also where operational experience and proven reliability performance reside
- A grid facing industry equals high likelihood of early response indications and warnings arising on the industry side

What should industry focus on going forward…

- Clarity on efforts to date
- Underscore authoritative findings to date
- Extend on efforts already underway
- Integrate the cross sector information sharing backplane
- Alignment compatibility to government threat fusion, regulatory communities, trades and other institutional partners
- Set the stage for rapid, collaborative mitigation development and delivery- automated decision support and information exchange

More focus items for industry…

- Taking a holistic, synergistic view towards the role of all resilience multiplier tools in the kit
- Improvement and innovation on how to collaborate with public sector
- Continued emphasis on SME contribution to influential initiatives and venues
- Keenly assertive work to accelerate the shift to risk informed, data driven and prioritized strategies
- Laser beam precision regarding performance based outcome orientation with a systems level lens

Industry activities supportive of response…

- Only sector, save Nuclear, with mandatory and enforceable Critical Infrastructure Protection standards
- Significant SME participation in collaboration initiatives, special topics (includes GMD and ES-C2M2, etc…)
- Assessment activity
- Educational and exercise events
- Collaborative standards development and tech vendor involvement
- Event Analysis and Reliability Performance Analysis, Risk-based, Data-driven
- Sector Coordination: ISAC, UCG, Cyber UCG
- ESF-12 and Regional Entity Support
- Mission Assurance, ES3P CIPAC Joint Working Group
- Implementation of an information sharing architectural vision
- Extensive CIPC Task Force Activity – Severe Impact Resiliency, Cyber Attack

NERC ES-ISAC Services and Products

- ES-ISAC Trend Report
- ES-ISAC portal for receipt of industry reporting, publishing threat guidance, sector coordination, operator self service tools and technical library
- ES-ISAC furnishes sector contingency coordination services at Unified Coordination Group (UCG, a federal government construct under National Response Framework/NIPP) level
- SME support to CRPA and Sufficiency Review industry assessment services
- SME participation in GridSecCon, GridEX and other key industry forums
- SME support to industry and government expert panels and development teams (such as ES-C2M2, IEEE, CIPC and others)
- ES-ISAC provides sector specific dynamic mitigation development and guidance in collaboration with vendors and the threat community (including governments, fusion cells and other sectors)
- ES-ISAC disseminates guidance through Alerts, Notices, Special Reports, and advanced portal services – ***Alerting with mandated feedback loop available***
- ES-ISAC maintains dynamic BPS risk understanding and common operational picture which correlates physical, cyber and operational wide area awareness

Where it is headed…

- Front-Mid-Back Plane Automated Information Sharing
- Risk driven strategies, applying prioritized effort
- Placing performance based outcomes metrics on those
- Attention to mutually supporting aspects of a balanced and holistic approach – how to lever for best resilience effect
- Alignment of public and private partner role and process definition

Unique Opportunities for Continued Industry Contribution

- Helping public sector identify and resolve gaps in capability extension of current constructs – UCG, NIPP, DSCA, Mission Assurance
- Assist public sector alignment goals with response community and energy sector structures
- Further assistance to sector level capability maturity
- Setting the stage for risk driven and automated information exchange approaches
- Organized, SME driven understanding of attack and vulnerability surfaces, mitigation development and delivery improvements
- Application of innovative ways to improve sector non-compliance security dialogue
- First mover contributor of sector indications and warnings, based on wide area awareness and operational expertise
- TTP development for quick, precise mitigation application