Monday, March 18	
9:00-9:15 am	*Welcome & Opening Remarks*
9:15-10:00 am	*Keynote* **The Cybersecurity and Infrastructure Security Agency's (CISA) Priorities in the Age of Convergence** CISA leads the national effort to *defend* critical infrastructure against the threats of *today*, while working with partners across all levels of government and in the private sector to *secure* against the evolving risks of *tomorrow*. Assistant Director Harrell will discuss what CISA is doing to coordinate security and resilience efforts, deliver training, technical assistance, and assessments to federal stakeholders as well as to infrastructure owners and operators nationwide. **Brian M. Harrell @CISAHarrell, Assistant Director for Infrastructure Security, Cybersecurity and Infrastructure Security Agency (CISA) Infrastructure Security Division, Dept. of Homeland Security**
10:00-10:30 am	Networking Break
10:30-11:15 am	**Evolution of ICS Attacks: From BlackEnergy2 to TRISIS** Cyber attacks on industrial control systems (ICS) were once sufficiently rare that years would pass with continued analysis of the same events. But since 2016 the pace of ICS-focused events has increased so dramatically that one event now seems to blur into another, with little time left to place each new incident (and its underlying methodology) into the context of the evolution of ICS attacks. This presentation seeks to address this gap by providing an overview of events ranging from the 2015 BlackEnergy2 grid attack in the Ukraine to CRASHOVERRIDE, the U.S./UK/German grid intrusions, and the TRISIS event. Two primary trends will be analyzed in detail: (1) The shift from custom malware in initial intrusion and entrenchment scenarios to increased dependence on system commands, scripts, and commodity malware; and (2) Increasing software and capability development moving technical proficiency away from on-keyboard operators and embedding ICS expertise in malware. These two seemingly conflicting trends underlie our experience as a community. The result has been an increase in efficiency in ICS-targeting operations, as initial attack phases begin to resemble traditional offensive operations (helped in no small part by the continued convergence of IT technology in OT environments) and final attack scenarios abstract away from the malicious individual to place all ICS-impacting functionality in purpose-built software. This has meant that a large number of malicious operations and actors can be supported by a relatively small number of specialized developers, lowering the overall cost of ICS intrusions and increasing the pace at which such operations can be executed.

	Joe Slowik @jfslowik, Adversary Hunter, Dragos
11:15-11:45 am	**Coordination, Cooperation, and Cyber-resilience: The Role of Energy Computer Emergency Response Teams in Offensive and Defensive Activities** Cooperation is one of the key elements of effective and efficient reaction to a cyber attack. The exchange of information about threats, vulnerabilities, and attacks provides organizations with the ability to quickly respond. A mature organization should have positions or teams responsible for cooperation, and indeed many institutions have a professional computer emergency response team that has Cyber Threat Intelligence among its competencies. In this presentation we'll talk about practical ways that cooperation and the exchange of information can be put in place help protect organizations from real danger and disasters in the energy sector. We have established cooperation at the national and international levels by creating a trusted network of organizations and people who can exchange information on a daily basis about threats and share details on how to protect IT or OT environments. That is the real added value of these contacts. **Jarek Sordyl, CISO/Head of CERT, PSE S.A.**
11:45 am – 1:00 pm	Lunch & Learn Sessions
1:00-1:45 pm	**CES-21 Technology Achievements: Grid Security and Cyber Automation** California Energy Systems for the 21st Century, known as CES-21, is a project led by California power generation companies and research partners to perform cutting-edge research to promote secure technologies across transmission and distribution infrastructure. Now in its fifth and final year, the project has produced some impressive technologies that will enable utility providers to improve their grid security posture, secure communications within industrial control systems (ICS), and ultimately provide a path towards automated security response. This talk will focus on the various technologies and protocols that are the core of CES-21's Machine to Machine Automated Threat Response. These technologies include utility-specific extensions to the STIX protocol that enable integration and communication of threats between utilities; a proposed ICS protocol that fully integrates encryption and authentication; and a working example of Quantum Key Distribution to facilitate broad key management. During this discussion, utility owners and operators can expect to hear about a sample of near-term technologies that will improve their security posture. Original equipment manufacturers and service providers will get a description of the future of integration of grid communications, and agencies will gain insight into private research that is benefiting the ICS community and national infrastructure as a whole. **Jon Taylor, Principal Cyber Security Consultant - SoCal Edison Technical Lead for CES-21, Revolutionary Security for Southern California Edison**

1:45-2:30 pm	**Practical Solutions to Supply Chain Attacks** This presentation will discuss the supply chain in terms of software and networks. We will examine various attacks on supply chains in industrial control systems and other industries that have occurred over the last few years. We'll then spend time looking at the various unsuccessful attempts by regulators and organizations to address these problems, followed by suggestions on how Emerson or other vendors can work with the end customer. **David Foose, Ovation Security Solutions Program Manager, Emerson**
2:30-3:00 pm	Networking Break
3:00-3:30 pm	**Scanners, Tunnels, and Sims, Oh My!** When it comes to testing and analyzing ICS communications in your lab, what is even better than getting your hands on tools from your engineers? Easy. Having your own set of tools, available for free, customized for your current needs, and extendable for your future needs. Welcome to the Control Things Tools project! Born out of the Control Things Platform, a Kali-esque distribution for ICS professionals, Control Things Tools attempts to bring these customizable tools directly to you. a separate but similar tool for each protocol and/or technology layer, complete with a simple to use python library for you to make (or contribute) your own such tools. Join us to explore the public release of the first series of these Control Things Tools: cti2c, ctspi, ctserial, ctip, ctmodbus, ctvelocio, and the python library that provides the command-line and graphical interfaces for these tools. **Justin Searle** @meeas**, Director of ICS Security, InGuardians; Senior Instructor, SANS Institute**
3:30-4:15 pm	**Securing the Distribution Grid: The State Regulatory Perspective** The NERC CIPS were created to help strengthen the security posture of the Bulk Electric System (BES), which includes large generation assets, control centers and high voltage transformers. While the well-being of the BES is critically important, the fact that the CIPS, for jurisdictional reasons, can't bring comparable levels of security to the lower voltage distribution grid - the elements of energy delivery infrastructure that transport electricity to business, bases and homes - is a big problem. Investor owned distribution utilities are under the purview of the public utility commissions (PUCs) of the states they serve, and each state operates its own regulatory structure, some with more sophisticated cybersecurity programs, some with less. It is clear that state regulatory structures must develop ways of meeting cybersecurity challenges, and that commissioners and staff must ensure

	their utilities are adhering to appropriate standards and conforming to best practices. Last year, together with support from the National Association of Regulatory Utility Commissioners (NARUC), Rachel, Andy, and SANS' Tim Conway conducted a highly successful pilot grid cybersecurity training program with the New England commissioners that will now be expanded to benefit other US regions. Rachel and Andy will present a few of the observations and lessons gathered from this experience. **Andy Bochman, Senior Grid Strategist, Idaho National Lab** **Rachel Goldwasser, Director of the New England Conference of Public Utility Commissioners (NECPUC)**
4:15-5:00 pm	**Creating a Security Metrics Program: How to Measure Programmatic Success** We've heard it all before: "Our team handles 500,000 cyber-attacks a day." "Cyber threats are increasing." "We track cybersecurity as a critical risk for our organization." But what does any of that really mean? Creating measurements and metrics around cybersecurity is difficult, but so is building a sustainable metrics program, regardless of the subject matter. Early tasks, including measuring what is important and resource management, can be undermined by external pressures to tell a certain narrative or prove certain results. How can our industry create unbiased, yet compelling, metrics? What is the right-sized team or amount of resources for a metrics program? Is such a program sustainable? This presentation will cover not only the basics of cybersecurity metrics, but also lay the foundation for how s security team can create a new metrics program that goes beyond red/yellow/green or compliance. By moving to objective and repeatable metrics, utility security leaders will be able to not only justify programmatic improvements, but also track trends across environments and future projects. With research from the U.S. Department of Energy, the Electric Power Research Institute, and the National Institute of Standards and Technology, practitioners can build a defensible security metrics program across strategic, tactical, and operational levels of the utility. **Jason Christopher, CTO, Axio Global, Inc.**
Tuesday, March 19	
9:00-10:00 am	Lifetime Achievement Award & Keynote
10:00-10:20 am	Networking Break
10:20-11:00 am	**Gaining Endpoint Log Visibility in ICS Environments** This presentation will discuss the reasons why it is important to gain visibility of logs on industrial control system endpoint devices, and examine

	different methods to achieve that visibility. We'll review different architectures and technology constraints involved in moving those logs to centralized IT/OT Security Information and Event Management from an oil and gas perspective. **Michael Hoffman, Principal ICS Security Engineer, Shell**
11:00-11:45 am	**Gaining Buy-in & Resources to Manage Cybersecurity Risk in OT Environments** This session will introduce and expand the concept of Risk Debt, which is the compounding relationship of technical and operational vulnerabilities on the cybersecurity posture of an environment, and the impact on ICS environments. We'll discuss use cases to highlight the importance of knowing existing mitigation measures and how they impact Risk Debt. You'll take away tips for better telling your own risk story, with a structured approach to answering "so what?" and examples of using this approach to communicate cyber risk to key stakeholders. **Samara Moore, Director – Cyber Strategy & Engagement, Exelon** **Jason Tugman, VP – Cyber Risk Engineering, Axio**
11:45 am – 1:00 pm	Networking Lunch & Vendor Expo
1:00-1:45 pm	**Assumed Breach Assessments: Using You Against You** Security assessments and penetration testing are performed by teams who you have allowed into your networks. But what happens when an attacker gains access to a user's workstation or an engineer's laptop? Do your security controls limit their actions on that system or within your network? Or can they go anywhere and do anything? This presentation will outline the aspects of an Assumed Breach Assessments. How can you prepare? What actions will the testing team do? What results should you expect? This way your team can evaluate what security efforts are effective and what needs improvement **Don C. Weber @cutaway, Principal Consultant, Founder, Cutaway Security, LLC**
1:45-2:15 pm	**ICS Risk Management Approaches: Vulnerability versus Threat versus Engineering, and What Works Best for You** There are a variety of different approaches, methods, and opinions as to how to best defend against industrial control system (ICS) cybersecurity threats. Some of the more popular approaches in the industry focus on vulnerabilities, threats, and engineering. This talk will walk through each of these approaches – that is, where they make sense, where things break down, and how asset owners can apply the approaches in their daily duties. Attendees will walk away with a better understanding of how these approaches can be best combined to strengthen their ICS program given

	the resource constraints (time, money, resources) faced by most asset owners. **Brian Proctor, Director, SecurityMatters** **Dr. Nathan Wallace, Director, Cybirical**
2:15-2:45 pm	**Intersection of Data Breach Notification and Critical Infrastructure Protection** Data breaches so common that the popular saying has it that there are two kinds of organizations: those who have been breached and those who just don't know it yet. But what happens once you're breached and you know it? Data breach notification involves a dizzying matrix of guidelines, regulatory mandates, corporate policy, and contractual obligations. We discuss things you might want to know before reporting a data breach as well as lessons learned from the aftermath of data breach notification. External reference cases as well and frontline experiences are reviewed. Observations suggest the intersection of data breach notification and critical infrastructure protection standards is complicated by supply chain scale and scope. **Bryan Owen, Principal Cyber Security Manager, OSISoft**
2:45-3:00 pm	Networking Break
3:00-3:30 pm	**Still bailing water out of my OT boat two years later** When I took over the Cyber Security Program for my company's generation fleet I felt like I had been promoted to captain of a ship. Things were going to be run my way, and we were going to be the pride of the utility sector. I quickly came to realize that I had been put in charge of a leaky OT boat run 10 year+ legacy systems, full of fundamental cyber security holes, and was given a solo cup to start bailing the water out. My two-year adventure has taught me a lot about how to pick up an OT cybersecurity program and chart a course to a brighter horizon. My talk will walk through the process I went through to analyze the program and lessons I have learned along the way. **Steven Briggs, Senior Program Manager I&C Systems Generation Cybersecurity (NERC CIP), Tennessee Valley Authority**
3:30-4:00 pm	**Preventing Your Physical Access Control System from Being Used Against You** In the world of ICS, physical access is king. Once physical access is gained to even a portion of the environment, attackers are able to bypass many network and endpoint protections. To defend against this threat, sophisticated physical access control systems are installed, but are often misconfigured and not used to their full potential. Even worse, some

	misconfigurations can turn a multi-million-dollar physical access control implementation into an attacker's best friend; allowing them to essentially become invisible to traditional detection methods. This session will provide the audience with a foundational understanding of a traditional physical security environment, demonstration of trending attacks, examples of common misconfigurations, and a roadmap to locking down deployed implementations. **Valerie Thomas @hacktress09, Executive Security Consultant, Securicon**
4:00-4:45 pm	**Industrial Cyber Threats and Issues in Attribution Across High Profile Attacks** Clustering adversary activity, or intrusions, into sets and groups is a useful practice to satisfy intelligence requirements related to cyber threats. However, the way we communicate about those threats can be distinct to schools of thought that form in the cyber threat intelligence community leading to issues when compared one for one. Additionally, some of this analysis lends itself to true attribution such as attributing attacks to governments. This can be a useful for strategic purposes but holds little value to the tactical level defender. When considering adversaries interested in industrial environments (ICS/IIoT) the attribution can be significant in its impact to politics or even insurance claims. This talk will explore some of the mistakes that have been made related to attribution of ICS attacks, perils of transitive attribution, it will explore concepts to drive more value to defenders through taking an intelligence driven approach, and it will leave the audience with an understanding of the adversaries behind some of the most prolific ICS attacks such as Ukraine 2016's power outage and TRISIS attack in Saudia Arabia and their activity since those attacks. **Robert M. Lee @robertmlee, Summit Co-Chair, SANS Institute**