Gary Ackerman is founder and executive director of the Western Power Trading Forum (WPTF), a mutual-bene t, non-pro t corporation. WPTF's mission is to encourage and promote lower electricity prices and enhanced system liability in policies undertaken either by the Federal Energy Regulatory Commission, California Independent System Operator, or the CPUC. WPTF's current membership of 70 entities includes generators, marketers, commodity traders, banks, retailers, and other major market participants in the Western-states electricity business. He has a BA in Economics from Michigan State University, and an MA in Economics from University of Chicago.

BACKGROUND

A recent report by the Department of Homeland Security identi- ed a 50 percent increase in the amount of cyber-attacks leveled against the energy industry in the past year; however, many more go unreported every year. As hackers grow more sophisticated and utilities, vendors, and customers continue to upgrade their infrastructure, the potential openings for hackers also increase. With more than 2,000 utilities across the country, 50 states, and a Federal government, there are many players with an opinion on what to do, and the industry faces many challenges and opportunities to address this issue. Several states, such as California, Michigan, Missouri, and Texas have increased their scrutiny over utility cybersecurity practices and protocols; in addition, the Federal government is also considering taking additional action (and jurisdiction) over the entirety of the electricity grid as it pertains to cybersecurity.

The sta of the CPUC issued a White Paper in September 2012 to consider what steps a regulatory body may take, and what issues a regulatory body should consider when considering cybersecurity requirements. In addition, the North American Electric Reliability Corporation, created in the wake of the 1968 blackouts, was enabled by Congress and the Federal Energy Regulatory Commission to be the reliability enforcement authority over the bulk power grid and has its own set of cybersecurity requirements. As utilities continue to modernize their infrastructure and vendors continue building "smarter" technology, regulators need to become more aware of impacts of new technology on utility operations, as well as the customer, and have some level of assurance that these new technologies do not ultimately disrupt the grid.

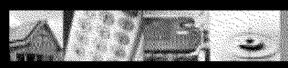
California Public Utilities Commission

Thought Leaders Series

#TL20

Wednesday, February 27, 2013
1:30 p.m. - 3:30 p.m.
CPUC Auditorium
505 Van Ness Avenue
San Francisco

1:30 p.m. - 1:35	Welcome to Thought Leaders
1:35 - 2	Opening Comments from Panelists
2 - 3	Interactive Dialogue between Panelists
3 - 3:20	Q&A with Audience
3:20 - 3:30	Closing Thoughts



Steven Dougherty is a Security and Privacy Architect with IBM's Global Business Services' (GBS) Global Center of Competency for Energy and Utilities. He is an experienced Cyber Security and Privacy Professional specializing in designing and implementing security & privacy architectures, security & privacy strategies and security & privacy governance, risk and compliance for Smart Grid and AMI infrastructures. With over 30 years experience serving the utility industry, his experience includes utilities in USA, Canada, Europe, Japan, South Africa, and Malta.

Tim Roxey is responsible for development and execution of key critical infrastructure protection initiatives, such as NERC's cybersecurity risk preparedness assessment and other continuous risk assessment e orts. Tim also acts as a key coordination point for North American government o cials and is the director of the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). Tim has over 30 years of experience in the nuclear utility industry serving in organizations such as Operations, Information Technology, Licensing, and Security, among others. Tim is a widely recognized leader in the elds of security and infrastructure protection, formerly serving as Deputy Chair of the Nuclear Sector Coordinating Council and Chairman of its Cyber Security Sub-Council. Tim is presently the Private Sector Chairman of the Industrial Controls System Joint Working Group (ICSJWG). He is also one of two co-chairs of the Cross Sector Cyber Security Working Group (CSCSWG).

James W. Sample is the Senior Director and Chief Information Security O cer at Paci c Gas and Electric Company. In this position James is accountable for leading, establishing, and maintaining company-wide governance, oversight, and support to identify and manage security risk and investment strategy to protect PG&E's critical infrastructure and information assets. Prior to joining PG&E, James was the Director of Enterprise Information Security and Policy for the Tennessee Valley Authority (TVA). In this role he was accountable for the governance, oversight, and support of TVAs enterprise information security program. James was directly responsible for the management of cybersecurity, privacy, and IT/OT risk management and compliance across all lines of business. James' experience also includes more than 8 years in leadership roles within the California Independent System Operator, 3 years with various consulting companies, and 6 years in the U. S. Navy.

Kevin Stine is the manager of the Security Outreach and Integration group within the National Institute of Standards and Technology's (NIST) Computer Security Division. e Security Outreach and Integration group develops, integrates, and promotes the mission-speci c application of information security standards, guidelines, best practices, and technologies. His work at NIST focuses on applying information security standards, practices, and technologies to the Health Information Technology sector; conducting outreach and awareness; and advancing security performance measurement. Kevin also serves as the chairperson of the Federal Computer Security Program Managers' Forum, an informal group sponsored by NIST to promote the sharing of information system security practices among federal agencies. Prior to joining NIST, Kevin served as the Chief Information Security O cer at the US Food and Drug Administrationy.