Cybersecurity and the Electric Grid: Innovation & Intellectual Property

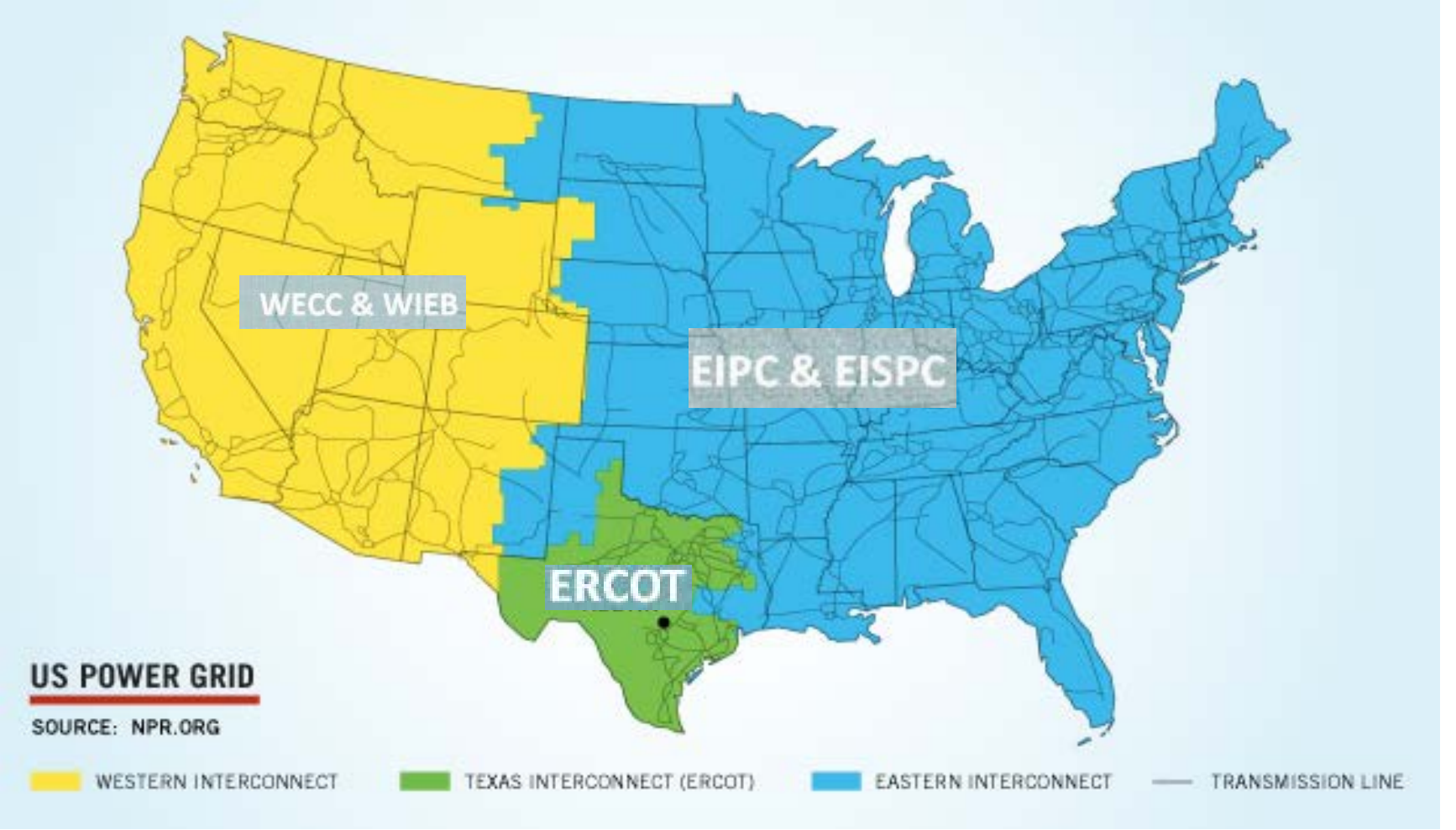
Theodore Wood, Esq.
Marc P. Dandin, PhD
30 May 2017

Wood IP LLC
555 Quince Orchard Rd, Suite 280
Gaithersburg MD, 20878

Overview

- The Electric Grid (basic structure)
- Needed Grid Enhancements
- Ecosystem for Developing Grid Enhancements
- Leveraging Intellectual Property (IP) to Enhance the Grid

The Grid (geographic view)



(Electricity Generation Sources)

	Coal	Petroleum Liquids	Petroleum Coke	Natural Gas	Other Gases	Nuclear	Renewables	Other	Total Generation (GWh)
2000	51.6%	2.7%	0.2%	15.8%	0.4%	19.8%	9.4%	0.1%	3,807,955
2001	50.8%	3.1%	0.3%	17.1%	0.2%	20.5%	7.7%	0.3%	3,745,745
2002	50.0%	2.0%	0.4%	17.9%	0.3%	20.2%	8.9%	0.3%	3,867,498
2003	50.7%	2.6%	0.4%	16.7%	0.4%	19.6%	9.1%	0.4%	3,892,115
2004	49.7%	2.5%	0.5%	17.8%	0.4%	19.8%	8.8%	0.4%	3,979,023
2005	49.5%	2.5%	0.6%	18.7%	0.3%	19.2%	8.8%	0.3%	4,062,458
2006	48.9%	1.1%	0.5%	20.1%	0.3%	19.3%	9.5%	0.3%	4,071,962
2007	48.4%	1.2%	0.4%	21.5%	0.3%	19.4%	8.5%	0.3%	4,164,748
2008	48.1%	0.8%	0.3%	21.4%	0.3%	19.5%	9.3%	0.3%	4,127,019
2009	44.4%	0.7%	0.3%	23.3%	0.3%	20.2%	10.6%	0.3%	3,956,990
2010	44.7%	0.6%	0.3%	23.9%	0.3%	19.5%	10.4%	0.3%	4,133,854
2011	42.2%	0.4%	0.3%	24.7%	0.3%	19.2%	12.6%	0.3%	4,112,181
2012	37.3%	0.3%	0.2%	30.3%	0.3%	18.9%	12.4%	0.3%	4,067,551
2013	38.9%	0.3%	0.3%	27.3%	0.3%	19.4%	13.1%	0.3%	4,074,457

U.S. Department of Energy, *2013 Renewable Energy Data Book*, December, 2014.

Trends

- Coal ↓
- Petroleum liquids ↓
- Nuclear —
- Renewables ↑

Electric Grid

- "The next Pearl Harbor is likely to be a cyber attack going after our grid…and that can literally cripple this country."
  (*Former CIA Director Leon Panetta*)
- Most important of the 17 DHS critical infrastructure sectors
- Critically outdated

How Outdated is the Grid?

Telephone

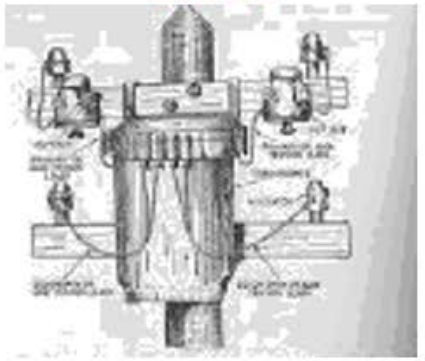
1876

Alexander Graham Bell's Invention

2017

Electric Grid

1882



Thomas Edison's Invention

2017

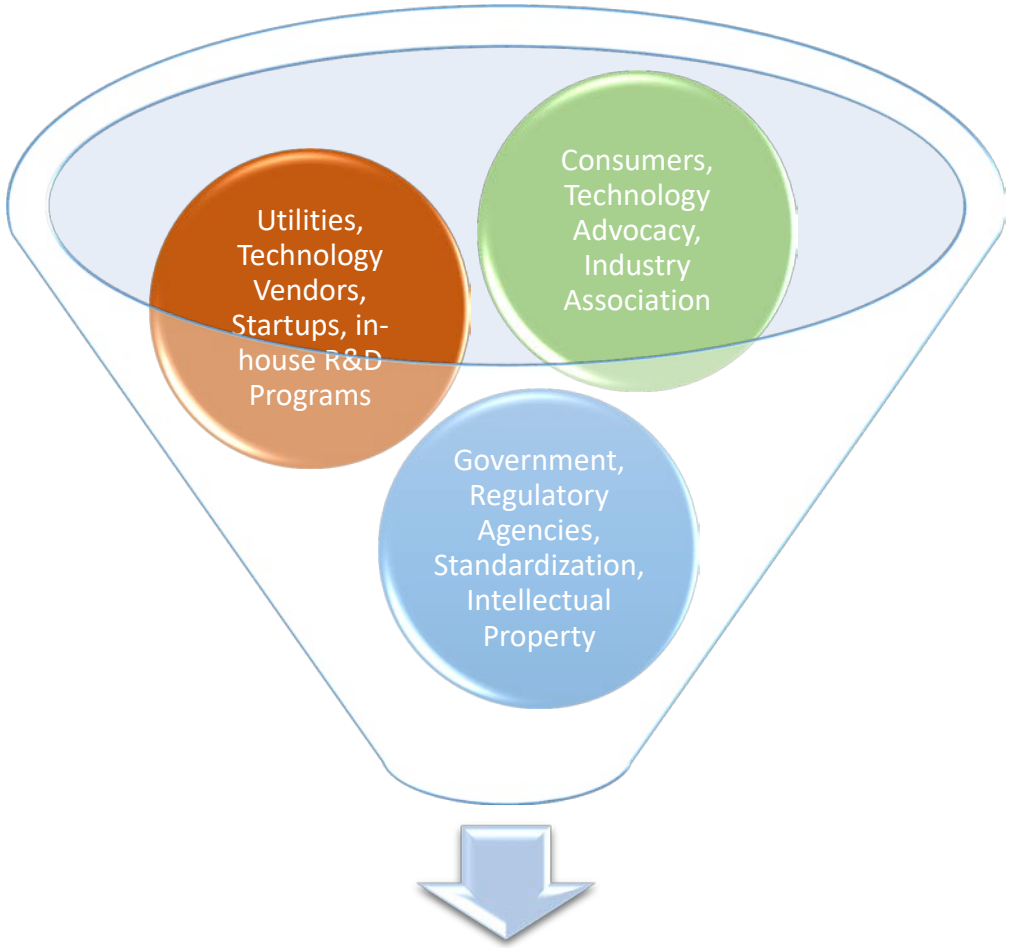
Critically Needed Upgrades

- Vulnerabilities:
  - Terrorism - physical infrastructure attack
  - Electromagnetic pulse (EMP)
  - Cyber attack
- Resiliency Enhancements

Grid Upgrade Technologies

A. Cyber (Hardware and Software) Resiliency Strategies	B. Power Grid Infrastructure Technologies	C. Physical Infrastructure Resiliency Strategies	D. Techniques for Validating and Certifying Grid Resiliency
1)Access Control 2)Authentication 3)Cryptography 4)Public Key Infrastructure (PKI) 5)Elliptic Curve Cryptography 6)Certificate Authority 7)Trust and Key Management 8)Software Upgrading 9)Patch Management 10)Rootkit Detection 11)Firewalls 12)DMZ (Demilitarized Zone) 13)Proxy 14)Network Access Control (NAC) 15)Anti Virus (AV) 16)Virtual Private Network (VPN) 17)Intrusion Detection System (IDS) 18)Intrusion Protection System (IPS) 19)Intrusion-Tolerance 20)Diversity Strategies 21)Replication Strategies 22)Intrusion Response System (IRS)	**SCADA Systems (Transmission & Operations)** 1)Intelligent Electronic Device (IED) 2)Remote Terminal Unit (RTU) 3)Programmable Logic Controller (PLC) 4)DNP-3 (Distributed Network Protocol 3) 5)MODBUS (serial communications protocol for PLCs) 6)IEC 61850 7)Inter-Control Center Communications Protocol (ICCP) 8)Energy Management System 9)Data Historian 10)Human Machine Interface (HMI) **Wide-area Measurement Systems** 1)GPS (Global Positioning System) Clock Synchronization 2)Phasor Measurement Unit (PMU) 3)Synchrophasors 4)Gateways 5)Phasor Data Concentrator (PDC) **Distribution Systems** 1)Advanced Metering Infrastructure (AMI) 2)Smart Meter 3)Meter Data Management System (MDMS) 4)Head End **Consumer-Area Energy Systems (Customer Oriented Technologies)**	1) Physical plant security 2) Grid physical component security 3) Data center facilities security 4) Security event detection and correlation 5) Electricity generation physical plant security 6) Substation physical security 7) Electric power transmission and distribution plant security 8) Grid decentralization strategies 9) Grid transformer and power line security 10) Microgrids 11) Physical threat resiliency strategies	1)Fuzzing 2)Penetration Testing 3)Red Teaming 4)Simulation 5)Validation Techniques 6)Verification Techniques 7)Conformance Testing 8)Modeling 9)Formal Proof 10) Modeling Checking **E. EMP Protection Technologies** 1) Robust Surge Protectors 2) Grounded Relay Houses 3) Shielded Power Supply Technologies 4) Neutral Blockers for Transformers 5) Coating Technologies 6) Control Room Shielding Technologies 7) EMP Protected Microgrids

Grid Development Ecosystem



Grid Enhancements

How are Patents relevant?

- ***Spur*** innovation
- Incentivize companies to engage in standardization
- Increase funding opportunities and market success for start-ups
- Increase security confidence of patented technologies

Challenges for Grid Technology Patents

- USPTO delays (pendency)
- Costs and uncertainties of patent protection
- Limited financial incentives for grid technologies
- Difficulties developing Standards Essential Patents (SEPs)
- Cybersecurity (Software-based) subject matter eligibility

Subject Matter Eligibility

- Patent statute (35 U.S.C. § 101):

  "Whoever invents or discovers any new and useful **process**, **machine**, **manufacture**, or **composition of matter**, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title."

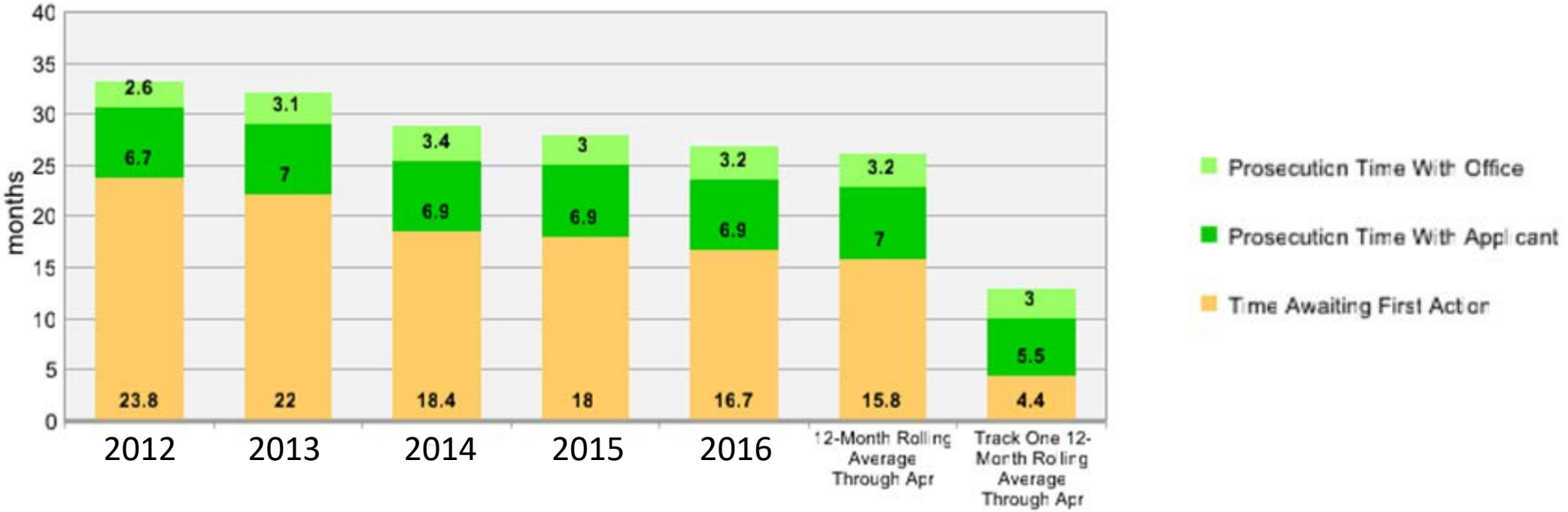
- ***Alice Corp. v. CLS Bank International***, 573 U.S. __, 134 S. Ct. 2347 (2014):
  - **Mere** implementation of a **conventional** method on a **computer** is abstract (not patent eligible)
- Cybersecurity patents may therefore be ineligible unless…

The Alice-proof Patent Application

(software related inventions)

- Describe special purpose computer *created* by the novel software
- Application-specific system beyond ‘mere implementation’ of a conventional idea on a computer
- Describe one part of the invention that *cannot* be performed without computer
- Describe *HOW* invention amounts to “significantly more” than abstract idea

Recommendation 1
(USPTO Application Pendency)



- USPTO should incentivize grid cybersecurity innovation by reducing cost of Track One petitions for related technologies

Recommendation 2

(IP Training for Cybersecurity Professionals)

- ***Universities*** should incorporate introductory IP courses in new cybersecurity programs

- ***Companies*** should implement basic IP training programs for inventors, especially in areas that pertain to cybersecurity patents

- ***Patent practitioners*** and ***companies*** should provide patent Examiners with Technology Training Seminars to improve quality of Cybersecurity patent examination

Recommendation 3
(Encourage Creation of SEPs)

- Companies should:
  - ❑ Embrace a collaborative R&D research model
  - ❑ Compete on products but ***collaborate*** on standards
  - ❑ Engage standard developing organizations early in development cycle (corollary to shortening patent examination)

Summary

- The Electric Grid (brief summary)
- Needed Grid Enhancements
- Ecosystem for Developing Grid Enhancements
- Leveraging IP to Enhance the Grid

Questions?

Theodore Wood Esq.
twood@woodiplaw.com
240-477-8581

Dr. Marc Dandin
mdandin@woodiplaw.com
240-912-7528

WOOD IP
CHANNELING INNOVATION

ISCAS 2017