We are with the Government, and We Are Here to Help!

- How and Why the Government is Taking Charge of Cybersecurity in Public Companies.

Guernsey, founded in 1928 in Oklahoma City provides a wide range of engineering, architecture, and consulting services.

We realize we're a little different. It's not often you'll see engineers and architects chatting over the water cooler - but then, it's not often you'll see an employee-owned firm that truly embodies what it means to be owned by employees, either.

Tim Fawcett is the Director of Cyber Security Consulting at Guernsey. Tim has over 20 years of information assurance experience performing IT audits, risk assessments, and cyber threat and vulnerability analyses. Over his career Tim has consulted for scores of companies from start-ups to Fortune 500 companies. In five years at Guernsey Tim has provided cyber security consulting dozen of companies including over 20 electric cooperatives and municipalities in ten states. Tim is a Certified Information Security Professional, a Certified Information Systems Auditor, and a CMMC Provisional Assessor Level 1 – 3.

Explorer operates a 1,830-mile common carrier pipeline that transports gasoline, diesel, fuel oil and jet fuel from the Gulf Coast to the Midwest. Through connections with other refined petroleum products pipelines, we serve more than 70 major cities in 16 states.

On our system, which has a capacity of 660,000 barrels a day, it takes as few as 11 days to move a barrel of product from the Gulf Coast region to the Chicago area.

With headquarters in Tulsa, Explorer is owned by Phillips66, Marathon, Sunoco Logistics and Shell.

Robert Martinez is the IT Security Administrator for Explorer Pipeline. In his time at Explorer Robert has overseen the significant improvements in Explorer 's cybersecurity program improving oversight and security for both the IT and OT environments.

Robert has extensive expertise in IT and cybersecurity operations having assisted with the development of scores of cybersecurity programs at organizations across many critical infrastructure industries.

Agenda

Cyber in the News

- SolarWinds
- Colonial Pipeline

Cybersecurity Legislation

Executive Action

- Identifying Critical Infrastructure
- TSA Security Directives for Pipelines
- DoD and CMMC

Agenda

Cyber in the News

- SolarWinds
- Colonial Pipeline

Cybersecurity Legislation

Executive Action

- Identifying Critical Infrastructure
- TSA Security Directives for Pipelines
- DoD and CMMC

Cybersecurity In the News

- Ransomware Attack On Alabama Hospital Caused Baby's Death
- Hackers Breached Colonial Pipeline Using Compromised Password
- The Bay Area and Oldsmar, Florida attack om water systems
- SolarWinds Breach

SolarWinds Attack – A Sophisticated Attack

Adam Meyers, vice president for threat intelligence at CrowdStrike, said when he became familiar with the SolarWinds attack, he knew it was a big deal. The technique reminded Meyers of old fears around trick-or-treating. For decades, there had been an urban myth that kids couldn't eat any Halloween candy before checking the wrapper seal because bad people might have put razor blades inside. What the hackers did with the code, Meyers said, was a little like that.

"Imagine those Reese's Peanut Butter Cups going into the package and just before the machine comes down and seals the package, some other thing comes in and slides a razor blade into your Reese's Peanut Butter Cup," he said. Instead of a razor blade, the hackers swapped the files so "the package gets sealed and it goes out the door to the store.“

Temple-Raston, D. (2021, April 16). *A 'worst nightmare' cyberattack: The untold story of the SolarWinds hack*. NPR. Retrieved October 5, 2021, from https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack.

Colonial Pipeline Ransomware Breach – A Not so Sophisticated Attack

1. Used a compromised Password found on the “Dark Web”
2. Used a VPN account that did not require MFA
3. The attack did NOT affect the Pipeline Control (OT network), Though at the time they did not know that at the time.
4. The pipeline was opened after physical inspection, because they have a safety culture
5. Colonial Pipeline operates gasoline pipelines, one step before upstream, they handle many more transactions.

Turton , W., & Mehrotra, K. (2021, June 4). *Hackers Breached Colonial Pipeline Using Compromised Password*. Bloomberg.com. Retrieved October 5, 2021, from https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password.

Agenda

Cyber in the News

- SolarWinds
- Colonial Pipeline

Cybersecurity Legislation

Executive Action

- Identifying Critical Infrastructure
- TSA Security Directives for Pipelines
- DoD and CMMC

Cybersecurity Legislation (Not including Privacy Laws)

At least 45 states and Puerto Rico introduced or considered more than 250 bills or resolutions that deal significantly with cybersecurity. Some of the issues seeing the most legislative activity include measures:

- Requiring government agencies to implement cybersecurity training, to set up and follow formal security policies, standards and practices, and to plan for and test how to respond to a security incident.
- Regulating cybersecurity within the insurance industry or addressing cybersecurity insurance.
- Creating task forces, councils or commissions to study or advise on cybersecurity issues.
- Supporting programs or incentives for cybersecurity training and education.

Oklahoma Passed Bills

2020 - OK S 1204 - Enacted - Relates to income tax, relates to income tax credit for qualifying software or cybersecurity employees, modifies definition, eliminates specific authority for participation in certain program and related requirements, updates statutory references, provides an effective date, declares an emergency.

2021 – Effective Nov. 1, 2021. An Act relating to crimes and punishments; which relate to the Oklahoma Computer Crimes Act; modifying definition; defining term; expanding scope of certain prohibited acts; making certain acts unlawful; providing construing provision; and providing an effective date.

Federal Cybersecurity Legislation

1. INVEST IN AMERICA ACT

The INVEST in America Act includes $600 million in funding to improve cybersecurity in the water, power, and transportation infrastructures, a $1 billion fund for state, local, and tribal governments to improve their security practices, and a provision for funding the new office of the National Cyber Director at a rate of $20 million annually through 2028.

2. AMERICAN RESCUE PLAN ACT

The American Rescue Plan Act included $1 billion for the Federal Technology Modernization fund (established in the Modernizing Government Technology Act of 2017). Act as a pool of funds that government agencies can use to apply for technology upgrade loans.

5. FOR THE PEOPLE ACT

The Democrat-led voting bill includes grants for voter system security improvements and imposes requirements on voting vendor companies including cybersecurity reporting and that the vendor companies be owned or controlled by United States citizens or permanent residents.

https://fiscalnote.com/blog/biggest-cybersecurity-policy-legislation-2021

Agenda

Cyber in the News

- SolarWinds
- Colonial Pipeline

Cybersecurity Legislation

Executive Action

- Identifying Critical Infrastructure
- TSA Security Directives for Pipelines
- DoD and CMMC

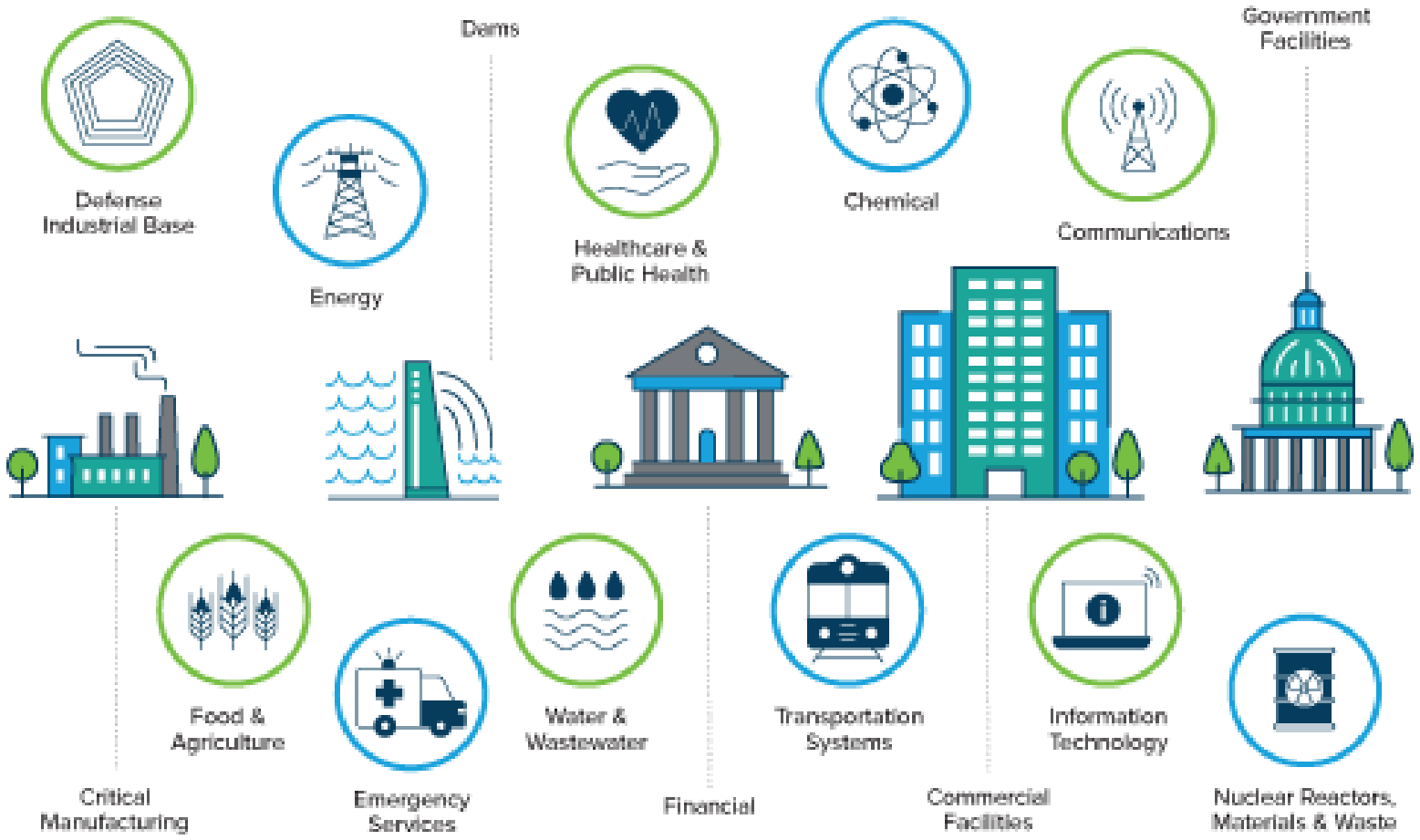
Executive Action

"When Congress refuses to act . . . I have an obligation as president to do what I can without them,"
President Obama - 2012.

explorer PIPELINE

guernsey

Essential Critical Infrastructure Workers



CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA

TSA Security Directive Pipeline-2021-01 (The May Directive)

On May 27, 2021, the Senior Official Performing the Duties of the TSA Administrator issued Security Directive Pipeline-2021-01 (security directive) requiring Owner/Operators of critical pipeline systems and facilities to take crucial measures to enhance pipeline cybersecurity. TSA issued this security directive in accordance with 49 U.S.C. 114(*l*)(2)(A), which authorizes TSA to issue emergency regulations or security directives without providing notice or public comment where "the Administrator determines that a regulation or security directive must be issued immediately in order to protect transportation security. . . ." TSA took this emergency action in response to the attack on Colonial Pipeline, which demonstrated the significant threat such attacks pose to the country's infrastructure and its national and economic security as a result. The directive became effective on May 28, 2021, and is set to expire on May 28, 2022.

Ratification of security directive. Federal Register. (2021, July 20). Retrieved October 5, 2021, from https://www.federalregister.gov/documents/2021/07/20/2021-15306/ratification-of-security-directive.

TSA Security Directive Pipeline-2021-02 (The July Directive)

The July Directive requires owners and operators of TSA-designated critical pipelines to implement specific mitigation measures to protect against ransomware attacks and other known threats to information technology and operational technology systems. Additionally, covered pipeline owners and operators must develop and implement a cybersecurity contingency and recovery plan, and conduct a cybersecurity architecture design review. Because the July Directive requires the covered pipeline owners and operators to implement specific cybersecurity practices, this directive is designated as "security sensitive," and a DHS spokesperson has reported that its distribution will be limited to those with a need to know.

Sinclair, B. (2021, July 26). *DHS pipes up again: Issues second directive on pipeline security*. JD Supra. Retrieved October 5, 2021, from https://www.jdsupra.com/legalnews/dhs-pipes-up-again-issues-second-2942405/.

CMMC – Defense Industrial Base

WHAT IS THE CMMC MODEL?

- Will be a requirement for all DoD contractors and Subcontractors in the next five years. (100,000 companies plus their contractors)
- “The CMMC Model combines various cybersecurity standards and best practices and maps the resulting controls and processes across several maturity levels that range from basic to advanced cyber hygiene.”
- The CMMC model encompasses the basic safeguarding requirements for protecting Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).
- Requires 3rd Party Certification
- 100% Conformity is the expected

CMMC PRACTICES

- Assigned to a specific CMMC level and domain
- Most practices from FAR and NIST 800-171

CMMC Level	CMMC Level Practices	Source			
		48 CFR 52.204-21	NIST SP 800-171r1	Draft NIST SP 800-171B	Other CMMC practices
Level 1	**17**	15	17	-	-
Level 2	**55**	-	48	-	7
Level 3	**58**	-	45	-	13
Level 4	**26**	-	-	11	15
Level 5	**15**	-	-	4	11
Total	**171**	**15**	**110**	**15**	**46**

Agenda

Cyber in the News

- SolarWinds
- Colonial Pipeline

Cybersecurity Legislation

Executive Action

- Identifying Critical Infrastructure
- TSA Security Directives for Pipelines
- DoD and CMMC

Guernsey can help you prepare for CMMC.

- Performing a pre-assessment for CMMC
- Help write policies and procedures
- Helping you develop an SSP and POA&M
- Design control activities that that are designed to create auditable artifacts
- Help implement controls or recommend best practices to pass CMMC

Guernsey is uniquely qualified to help with CMMC compliance.

- Guernsey is a DoD contractor and subject to CMMC
- Guernsey does not sell managed services, compliance platforms, or software
- We are certified auditors and security professionals
- We are centrally located
- We have been in business for over 92 years providing services to regulated industries and small to mid-sized organizations
- We are an RPO and C3PAO