[Company Name]

[Company Address]
[City, ST ZIP Code]

ICS Cyber Security Plan of Action & Milestones (POA&M) Roadmap

Date	Services Performed By:	Services Performed For:
[Date]	[Company Name] [Company Address] [City, ST ZIP Code]	Customer Address

Insert picture of customer critical field Asset here

POA&M Interview Dates:
Month Day to Month Day Year
Report Date:
Month Day Year

Disclaimer

This document has been prepared in good faith based on information available at the date of publication without any independent verification. We do not guarantee or guarantee the accuracy, reliability, or completeness of the information in this publication nor its usefulness in achieving any purpose. This document is prepared for information purposes only. Readers are responsible for assessing the relevance and accuracy of the content of this publication. We will not be liable for any loss, damage, cost, or expense incurred or arising by reason of any person using or relying on information in this document. By accessing this document, you acknowledge, accept, and agree to the foregoing.

About Consultant

Consultant is a security services consulting company focused on critical infrastructure sectors that own, operate, and depend on industrial control systems (ICS), automation systems,

process control systems, SCADA, DCS, PLC, RTU, safety instrumented systems (SIS) and other operational technologies (OT) and cyber-physical systems (CPS). With global experiences across various asset types and verticals such as water, wastewater, electric, oil, gas, manufacturing, maritime and building automation, both in government, including military and private sector Consultant is best positioned to provide security services to asset owners, operators, EPCs, integrators, larger consulting firms, and OEMs. For more information, visit contact us at

Table of Contents

Executive Summary

Customer XYZ engaged Consultant to provide a road map with plans of actions and milestones (POA&M) towards improving the security of critical operations that use industrial control systems, automation systems and operational technologies also known as ICS/OT. Consultant spent a week at Customer XYZ during **(date range)** at **(sites)** conducting some discovery interviews and a one-day field **(could be more than one day)** visit to **types of critical assets** to get an initial view of Customer ’s operations and ICS/OT footprint. During our visit we also provided immediate advice to the **who? List roles, parts of organization etc**. This roadmap and POA&M report contains some prioritization of key observations and recommended mitigations, some criticality ratings for ICS/OT focused assets and timeline of mitigation tasks with a detailed appendix of tasks and recommendations on ICS security focused trainings, certifications and roles and responsibilities.

Viewing an example of multiple critical asset types and site locations contributed to consultant understanding of the detailed context of the challenges that **Customer** faces with securing its critical infrastructure. To gain further insight to the possible people and process opposition Customer faces with securing the ICS infrastructure, Consultant met with the **who?** to gain knowledge of any hurdles you may face **from what and who?** despite having Customer board-level support. However, this POA&M roadmap focuses primarily on the current state of the technology, operations, and roles in use in Customer ’s critical infrastructure with a roadmap guide towards a potential future state of where Customer could be for ICS/OT security.

CONSULTANT has prepared initial high-level guidance and recommendations for Customer to begin to prioritize and address critical gaps in the ICS computing and operational environment. In addition, CONSULTANT has recommended guidance information that is prioritized to address deficiencies that will better align to cybersecurity and risk management programs as defined by industry standard architectural solutions that comply with the Secure Architecture for Industrial Control Systems of separating each industrial computing level as well as securing ICS system control structure according to ISA/IEC-62443. Further, the POA&M roadmap contains key observations coupled with recommended mitigations, some criticality ratings for ICS/OT focused assets and timeline of mitigation tasks. The Appendix Section also has recommendations on ICS security-focused trainings, certifications and roles and responsibilities to further help Customer address any gaps identified in this POA&M.

Outside the scope of this assessment is the review of Customer ’s business network or information technology (IT) security, which consequently removes any recommendations or conclusions to converge IT security practices with ICS/OT security.

Background Information

Customer, Inc. is an independent oil and natural gas company, which engages in the acquisition, development and exploration of oil and natural gas properties. Its operations are focused in the Permian Basin region of Southeast New Mexico and West Texas. The company's core operating areas include XYZ. The company was founded on XYZ and is headquartered in Location XYZ.

As of XYZ, its total estimated proved reserves were ### million barrels of oil equivalent. As of the end of Q1 YEAR, Customer reported total operating revenues of $$$ million against $$$ million a year ago. Income from operations was $$$$ million against $$$$ million a year ago. Income before income taxes was $$$$ million against $$$$ million a year ago. Net income was $$$$ million or $$$$ per diluted share against $$$$ million or $$$$ per diluted share a year ago. Net cash provided by operating activities was $$$$ million against $$$$ million a year ago.

Project Scope

This site security assessment was structured to review all Customer ICS/OT assets, the typical network architecture of the assets, standard connectivity to the ICS/OT assets, review of roles and operational practices and a review of the physical security of some Customer ICS/OT field assets. Also included were security reviews of the configurations of any equipment that typically participates in the makeup of the ICS/OT computing environment, particularly the communications equipment used by ICS/OT assets and operations. Security Process reviews were included to understand overall security posture of the ICS/OT environment. This includes any asset management reviews, security monitoring reviews, security policy reviews, security process reviews, 3rd Party Management process reviews, and process control reviews pertaining the ICS/OT computing environment.

Project Contacts:

The following Customer and CONSULTANT Cyber Security personnel have been directly involved in the execution of this cyber security program assessment:

Name	Project Role	Organization

		CONSULTANT Cyber Security
		CONSULTANT Cyber Security
		CONSULTANT Cyber Security
		CONSULTANT Cyber Security
		Customer, Inc
		Customer, Inc

Any questions, comments, or feedback related to the content of this report should be submitted to the primary CONSULTANT assessment and mitigation lead.

Key Findings & Mitigations

The table below highlights some of the key observations or findings our team discovered during our one-week visit. Each finding has at least one or more associated mitigation POA&M task ID numbers and a status of if our team agreed that the task is urgent meaning it needs to be initiated within the next 90 days, short-term needs to be initiated in 6 months or long-term needs to be initiated within 12 months or more. Keep in mind our recommendation to initiate certain tasks does not imply they will be completed within that same time frame. See the detailed POA&M task ID # in Appendix 1, this will give a specific estimated time it would take to complete a specific task. Tasks can be completed in whichever order Customer decides but we recommend kicking off the Urgent and Short-term tasks as soon as possible.

Key Findings	Mitigations	Status
No logging of network traffic from downstream in the field being sent back upstream to Claroty ICS protocol monitoring platform	POA&M task ID # 11	Urgent
No RF/Wireless intrusion detection or prevention solution being used for most critical wells, tank	POA&M task ID # 14, 18	Short-term

batteries, or saltwater disposal sites		
No enablement or centralized collection of syslog from devices that can support it	POA&M task ID # 11, 14, 18	Urgent
No firewalls and zone segmented access control lists implemented on RF/wireless assets such as Cambium, MDS INET and Netonix	POA&M task ID # 3, 11, 12, 14, 17, 18	Urgent
No ability to confirm that Freewave devices are communicating with each other through encrypted connections	POA&M task ID # 18	Urgent
No syslog, monitoring, or firewall capability able to be confirmed in Freewave devices	POA&M task ID # 18	Urgent
No implementation of security zones and conduits or industrial firewalls and unidirectional gateways out in the field, third party and connected back into corporate IT networks (e.g., servers on business network can poll downstream through the architecture directly to controllers in the field using protocols like OPC and Modbus)	POA&M task ID # 3, 11, 14, 18	Short-term
No ICS Change or Configuration Control Board (CCB) that	POA&M task ID # 2, 4, 5, 15, 16	Urgent

includes Facilities Management, Construction Management, Automation Superintendent, IT, Cybersecurity, Physical Security and Procurement for third party management		
No ICS security requirements being uniformly enforced with all third parties such as breach notification, delivery of commissioning guides, factory or site acceptance testing (FAT/SAT) procedures, device manuals etc	POA&M task ID # 2, 4, 5, 15, 16, 20	Short-term
No ICS Security Program Manager and Governance council to include the Automation Superintendent, Facilities, Physical Security, Construction, IT, security, Telecom, Contracting, HR, and Safety	POA&M task ID # 2, 4, 5, 8, 23, 27, 28, 29	Urgent
No ICS focused Cybersecurity training, awareness, and certification program	POA&M task ID # 1	Short-term
No ICS focused Incident Response Program with ICS security trained personnel (e.g., including communications plan with ICS-CERT, third	POA&M task ID # 7	Short-term

parties, reporting of suspicious activity or visitors near sites etc		
No formalized ICS business continuity, DRP or Contingency Plans, processes, procedures in place (e.g., for tank batteries, wells, saltwater disposal)	POA&M task ID # 6	Short-term
No consistent or coordinated collaboration and agreements with ICS/OT vendors, integrators, and contractors to upgrade and continuously maintain ICS/OT assets	POA&M task ID # 2, 3, 4, 10, 15, 16	Short-term
No ICS focused annual assessments and penetration tests from independent third-party testers with ICS security and ICS field operations experience to include consequence, impact and threat analysis and modeling	POA&M task ID # 21, 26, 27	Long-term
No required accreditation and certification of ICS/OT systems, devices, and network security (e.g., ISA/IEC 62443 ISA Secure certification, UL 2900 certification)	POA&M task ID # 2	Long-term
No documented system security plans and configuration plans, engineering	POA&M task ID # 2, 3, 4, 20	Long-term

diagrams of ICS devices, systems, applications, and networks		
No ICS personnel check in to check out systems in place to enforce lifecycle personal management including roles, responsibilities, and need for access to ICS and field operations (e.g., third-parties, transient employees etc)	POA&M task ID # 1, 10, 13, 23, 29	Short-term
No formal test and development lab and centralized parts management program for ICS assets	POA&M task ID # 6, 24	Short-term
No centralized ICS asset management and inventory tracking and control capability implemented (e.g., FactoryTalk for all Allen Bradley-Rockwell family of PLCs and HMIs and their connected sensors etc)	POA&M task ID # 4	Long-term
No laptop and portable media chain of custody, sign in and sign out or malware sandbox texting (e.g., Cuckoo, Remnux, Volatility) implemented or enforced for ICS (e.g., when engineers or third parties need to connect USB, CD/DVD, laptop, tablet, or	POA&M task ID # 19	Long-term

phone to an ICS device).		
No required maintenance window for system updates, upgrades, testing and patches both internal to the company or external requirements for third parties	POA&M task ID # 2, 5, 16	Long-term
No complete awareness, visibility or contract control over all assets that could be talking out to the internet or have direct third-party remote control	POA&M task ID # 2, 5, 15, 22, 29	Urgent
Limited visibility and controls implemented to control physical access to field sites and equipment	POA&M task ID # 2, 5, 9, 10, 13, 19	Urgent

ICS/OT Systems Impact Assessment

We recommend conducting confidentiality, integrity and availability (CIA) impact assessments for each system type critical ICS asset or ICS supporting asset to enable Customer to prioritize mitigation measures. The following table contains some of the critical assets and devices we identified during our one-week interview. The table is not an exhaustive list but an example of an impact assessment exercise that we recommend Customer undertake for each type of critical ICS or ICS supporting asset as the maturity level of the company wide ICS security program grows overtime.

Potential Impact	Definition	In Practice

Low	The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on company and ICS, organizational assets, or individuals	A limited adverse effect means that a security breach might: (i) cause a degradation in ICS operation to an extent and duration that the organization can perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Moderate	The loss of confidentiality, integrity, or availability could be expected to have a substantial adverse effect on company and ICS, company and ICS assets, or individuals	A substantial adverse effect means that a security breach might: (i) cause a significant degradation in ICS operation to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv), result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.
HIGH	THE LOSS OF CONFIDENTIALITY, INTEGRITY, OR AVAILABILITY COULD BE EXPECTED TO HAVE A SEVERE OR CATASTROPHIC ADVERSE EFFECT ON COMPANY AND ICS OPERATIONS, COMPANY AND ICS ASSETS, OR INDIVIDUALS.	A SEVERE OR CATASTROPHIC ADVERSE EFFECT MEANS THAT A SECURITY BREACH MIGHT: (I) CAUSE A SEVERE DEGRADATION IN OR LOSS OF ICS OPERATION TO AN EXTENT AND DURATION THAT THE ORGANIZATION IS NOT ABLE TO PERFORM ONE OR MORE OF ITS PRIMARY FUNCTIONS; (II) RESULT IN MAJOR DAMAGE TO ORGANIZATIONAL ASSETS; (III) RESULT IN MAJOR FINANCIAL LOSS; OR (IV) RESULT IN SEVERE OR CATASTROPHIC HARM TO INDIVIDUALS INVOLVING LOSS OF LIFE OR SERIOUS LIFE• THREATENING INJURIES.

See table below for more information about the definition of potential impacts. The overall rating is using the highest watermark approach where the highest impact rating of either confidentiality, integrity or availability warrants giving an asset overall rating of the highest of the three. The impact levels of assets can change based on how the asset is being used and its level of usage by or impact to ICS devices, personnel, and operations.

Site Type	Asset	Confidentiality	Integrity	Availability	Overall

Well	Lufkin Pump Off Controller (POC)	Low	High	High	High
Tank Battery	MDS INET	Medium	Medium	High	High
Tank Battery	RedLion HMI	Low	High	High	High
Tank Battery	Phoenix Contact PLC	Low	High	High	High
Wells	Cambium ePMP 1000 Access Point & Force 180 Radios	Medium	High	High	High
	Rockwell-Allen Bradley PLCs	Low	High	High	High
	Moxa serial converter	Low	Medium	High	High
	DigiPort serial converter	Low	High	High	High
	Kepware	Medium	Medium	Medium	Medium
	XSPOC	Medium	Medium	Medium	Medium
	ICS/OT routers	Medium	High	High	High
	DMZ 25 Firewall	High	High	High	High
	Lenel physical access card reader/keypad	Medium	High	Medium	High
	HID access card reader/keypad	Medium	High	Medium	High
	JACE building controller	Low	Medium	Medium	Medium
	Freewave Master & Slave radios	High	High	Medium	High
	IDEC HMI	Low	High	High	High

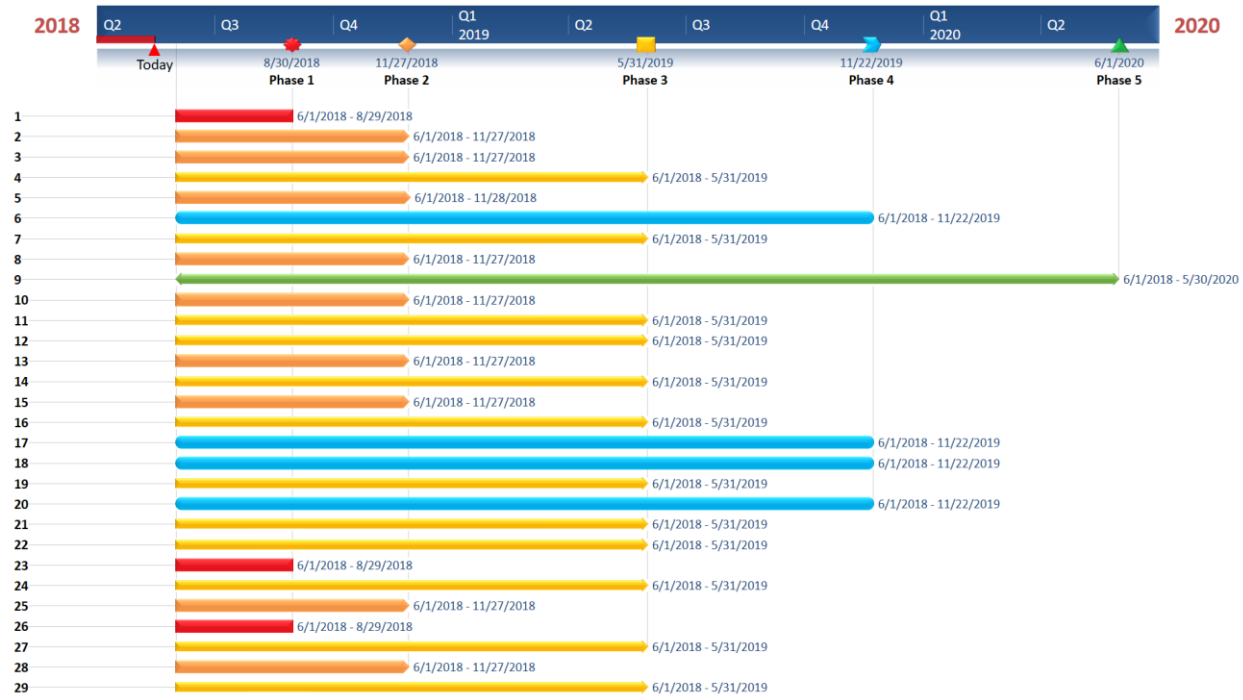
	Electric Reclosers	Low	High	High	High
	Electric substation	Low	High	High	High
	CCTV Cameras	Medium	Medium	Medium	Medium
	Chillers	Low	Medium	Medium	Medium
	BACnet serial converter	Low	Medium	Medium	Medium
	Netonix Wireless ISP	Medium	Medium	High	High

Execution Phase Timeline

Below is an example execution phase timeline chart based on the tasks we have outlined within Appendix 1. For purposes of illustration, we kicked off all the tasks with the same start date of Month Day Year. The Tasks are broken up into color coded phases based on estimated time to complete the task. These time estimations assume that dedicated resources will be assigned to each task. The sample start date does not imply that the tasks must be started at the same time. The estimated time to complete the task is estimated based on how long it should take to complete the task with dedicated resources from whatever the actual start date of the specific task is.

The following color-coded timeline shows which phase each POA&M ID # falls into:

	Phase One tasks with estimated completion within 90 days
	Phase Two tasks with estimated completion within 6 months
	Phase Three tasks with estimated completion within 12 months
	Phase Four tasks with estimated completion within 18 months
	Phase Five tasks with estimated completion within 24 months or more



Conclusion

Overall, from a strategic and program-level perspective related to securing Customer's ICS/OT operational environment, Customer's risk and governance of the ICS/OT environment is insufficient and represents a significant risk to personnel safety and the environment should a cyber incident occur. Given that basic visibility into the ICS/OT network is inadequate and is not segregated from the IT business network properly, unmonitored cyber events in the ICS/OT network potentially go undetected. Consequently, not complying with the Secure Architecture for Industrial Control Systems of separating each industrial computing level as well as securing ICS system control structure according to ISA/IEC 62443 represents significant risk to both Customer's IT data as well as Customer's ICS/OT processes.

For Customer to reach a more mature level of security within ICS/OT assets and field operations, CONSULTANT's ICS Plan of Actions & Milestones (POA&M)/ICS Security Roadmap should be utilized as a roadmap guiding Customer through a multi-step, multi-year plan to address both governance issues as well as technical issues. The roadmap should be implemented as a whole, which includes implementing both risk and governance processes as well as implementing new technology and architecture. Complying with CONSULTANT's recommendations clearly requires cooperation from both Customer's corporate IT Security personnel and Operations Asset Owners. In CONSULTANT's

experience, without cooperation from both parties, improvement in securing the business enterprise across both IT and ICS/OT assets is impossible.

In short, CONSULTANT recommends that Customer leadership allocate sufficient resources, budget, and personnel to both facilitate remediation of cyber security governance, risk management program, and capability deficiencies in the ICS/OT environment, as well as provide for effective management and maintenance of the program over time. Addressing program deficiencies identified may require adoption/replacement of new technologies and additional personnel, 3rd Party support resources, as determined by remediation and ongoing cyber security program management strategies.

Appendix 1: Plan of Action & Milestones (POA&M)

Plans of Action & Milestones are used in the critical infrastructure sectors to create and track execution plans needed to mitigate existing and ongoing risk to the organization, its people, its assets, and its operations. Tasks are not arranged in any order of priority in the appendix. However, the Execution Phase Timeline and key findings rank tasks in order of recommended phase priority. Each task's estimated completion time as well as real world start time can be adjusted based on company resources both contracted third-party expertise and organic resources including budget and dedicated personnel to the task. This POA&M services as a technical yet multiyear strategic roadmap focused on the key improvements and capabilities needed to have the largest positive impact to operational resilience and ICS/OT security. For the sake of visual mapping all tasks regardless of recommended urgency to initiate have the same generic start date of 6/1/2018 on the visual execution phase timeline.

TASK ID #:	Start Date:	Finish Date:	EST. TIME TO FINISH:	PHASE:
1			90 days	1
ROLES/RESOURCES:		Automation Engineer, IT/CIO, ICS Security Engineer/Manager, IT Security Staff, CISO, Facilities Manager/Construction Project Manager, Physical Security, Contract Management Staff, ICS OEM Vendor, Contractor, Integrator/EPC, ICS Security services firm, Automation Superintendent, Asset Owner VPs		

TASK: Create enterprise training policy and procedures that address ICS/OT specific needs. Include required technical training for key roles and executive level training for management. Appendix 2 provides some ICS/OT focused security trainings from sources such as ICS-CERT**,** SCADAHacker**,** Cybatiworks**,** ISA and SANS ICS**.** CONSULTANT also offers a ThreatGEN gaming style red team/blue team training to teach some ICS/OT security principals for both technical and non-technical audiences in one day. Also ensure enterprise training to all personnel for general awareness at least annually. Ensure ICS/OT security roles and responsibilities are addressed. Ensure field offices and zones can operate in the event they cannot receive timely support from a centralized corporate based operations team. This should also be T**AKEN** into consideration adding such requirements into contractor, integrator**,** and vendor agreements as well.

TASK ID #:	Start Date:	Finish Date:	EST. TIME TO FINISH:	PHASE:
2			6 months	2
ROLES/RESOURCES:		Automation Engineer, IT/CIO, ICS Security Engineer/Manager, IT Security Staff, CISO, Facilities Manager/Construction Project Manager, Physical Security, Contract Management Staff, ICS OEM Vendor, Contractor, Integrator/EPC, ICS Security services firm, Automation Superintendent, Asset Owner VPs		

TASK: Develop security contract language requirements, procedures**,** and templates to be used by all brands for all ICS assets**.** Evaluate security controls from ISA/IEC 62443 and NIST SP 800-82 to include in a security section for all projects and contracts with ICS/OT related assets**.** Require third parties to provide, where feasible ISA/IEC 62443 and or UL 2900 certified assets within their inventory and system design. Use ISO/IEC 27001 and NIST SP 800-53 for all IT assets supporting ICS or with connections to ICS**.** Ensure contracts include third-party independent security testers/validators that report their findings back to the Automation Superintendent, CISO, CIO, Facilities Management, Safety, Physical Security**,** and operational VPs or are asset owners within the company**.** Ensure contract language covers breach notification, right to audit, training, spare parts, business continuity, patching, continuous maintenance, site view coordination, visibility**,** and control over remote services such as time based and scheduled session controlled based access etc. This mitigates examples such as third-parties (in this case "Integrator/EPC/OEM") showing up at Mabee site X tank battery and lack unit location without first checking in with the field office through controlled access on May 3, 2018 and the day after they were onsite, on May 4, 2018 the Customer automation engineers visit the site only to see that all set points and configurations for the pumps within the Red Lion HMI and Phoenix Contact I/O controller have been wiped with no record of who did it. The third party also left behind an embedded micro computing device known as a Beaglebone to pull I/O data and they have an unsecure cellular modem plugged into an unmanaged switch talking unmonitored to and from controllers in the panel box. These sorts of events happen in every sector more often than most can capture and document them without implementing such controls in contract language then leveraging technologies such as Xona Systems to enforce third party access control for example.

TASK ID #:	Start Date:	Finish Date:	EST. TIME TO FINISH:	PHASE:
3			6 months	2
ROLES/RESOURCES:		Automation Engineer, IT/CIO, ICS Security Engineer/Manager, IT Security Staff, CISO, Facilities Manager/Construction Project Manager, Physical Security, Contract Management Staff, ICS OEM Vendor, Contractor, Integrator/EPC, ICS Security services firm, Automation Superintendent,		

	Asset Owner VPs
TASK: Create procedures and templates that show and enforce example diagrams and technical requirements of properly segmented networks, security zones**,** and conduits. Ensure all procedures and diagrams point to a policy requiring such implementation approaches for all ICS/OT assets. Ensure standardization of icons, legend color codes for Communications types, conduit types**,** and protocol types especially for ICS/OT assets and any connections to and from ICS/OT assets. Ensure these requirements are also placed into contracts and enforced upon third parties as well. This enables updated mapping documentation of all conduits and zones within and between zones to and from ICS/OT assets across the enterprise regardless of where they are located (e.g.**,** HVAC, Fire in Corporate or Pump Off Controller at a Well).	

TASK ID #:	Start Date:	Finish Date:	EST. TIME TO FINISH:	PHASE:
4			12 months	3
ROLES/RESOURCES:		Automation Engineer, IT/CIO, ICS Security Engineer/Manager, IT Security Staff, CISO, Facilities Manager/Construction Project Manager, Physical Security, Contract Management Staff, ICS OEM Vendor, Contractor, Integrator/EPC, ICS Security services firm, Automation Superintendent, Asset Owner VPs		
TASK: Create policy, procedures and templates for asset and inventory management that track type of device, name of device, asset tag, ports, protocols, services, software, hardware, licenses, conduit and communications type, brand, ICS/OT, system owner, date of installs, installed by, inspected and tested by date of test etc. Ensure this information is also enforced in contract language security specifications as well. All vendors, integrators and EPCs need to provide this information as part of the project deliverables and must support in maintaining the accuracy of the information. Additionally, seek out ICS focused solutions that are compatible with most of the controllers and assets in use such as Rockwell-Allen Bradley's Factory Talk suite that provides these capabilities for all assets in their brand as well as common competitor brands often used by their customer base. Ensure template configuration management plans and system security plans at the system level (e.g.**,** process control network, DMZ, PLCs for Wells, PLCs for tank batteries etc) document the security controls implemented, the functional and security features of the system.				

TASK ID #:	Start Date:	Finish Date:	EST. TIME TO FINISH:	PHASE:
5			6 months	2
ROLES/RESOURCES:		Automation Engineer, IT/CIO, ICS Security Engineer/Manager, IT Security Staff, CISO, Facilities Manager/Construction Project Manager, Physical Security, Contract Management Staff, ICS OEM Vendor, Contractor, Integrator/EPC, ICS Security services firm, Automation Superintendent, Asset Owner VPs		

TASK: Create ICS configuration management council and ICS change control board (CCB) with key member stakeholders such as CIO, VPs of each operational area, Facilities Management, Construction Management, Safety, Physical Security, Automation Superintendent, IT Security, ICS Security. The Executive Council will provide strategic direction, contractual leverage over third parties and the technical level CCB will provide detailed control over factory acceptance testing (FAT), site acceptance testing (SAT), Commissioning, patching, labs, spare parts, and other technical lifecycle issues focused on ICS/OT assets. The council and CCB should build enforcing contract agreements, policies, and procedures. Special procedures for ICS/OT should also be defined for test environments used to regularly test patching from vendors, enforce usage of company owned, provided and scanned laptops, USB, external drives, cd/DVD, custom maintenance windows for vulnerability scanning in test environments and during life cycle of assets not blindly on ICS/OT production networks. Procedures should also include monthly control council meetings at the management and executive levels and follow-up CCB meetings at the technical level for each project or asset. Configurations should address account management, password management and rigor, role, and attribute-based access (for humans, services, and technologies), turning off services not needed and using secure protocols and services like SSH instead of telnet. Requirements should also be placed on vendors in contract to provide proof of testing that they could not modify firmware on devices to support more secure services such as SSH, SCP, sftp and the disabling of ftp, telnet, and other insecure features. Ensure responsible ICS/OT personnel can operate, troubleshoot, and maintain secure configuration requirements in the event that timely and sufficient corporate or third-party based support is not possible or feasible.

TASK ID #:	Start Date:	Finish Date:	EST. TIME TO FINISH:	PHASE:
6			18 months	4
ROLES/RESOURCES:		Automation Engineer, IT/CIO, ICS Security Engineer/Manager, IT Security Staff, CISO, Facilities Manager/Construction Project Manager, Physical Security, Contract Management Staff, ICS OEM Vendor, Contractor, Integrator/EPC, ICS Security services firm, Automation Superintendent, Asset Owner VPs		

TASK: Leverage NIST CSF, NIST SP 800-82, 53 & 34 and ISA/IEC 99/62443 to create contingency, disaster recovery and business continuity plans, policies, and procedures for each ICS system to include asset type, asset region, operation, brand. Ensure specific ICS/OT procedures are included in dedicated sections leveraging recommendations from ICS-CERT, US CYBERCOM, NIST, ISA and oil and gas organizations such as AGA and INGAA. Ensure system level procedures and plans roll up into regional, site and enterprise wide plans and procedures. Ensure procedures include creation, testing and sustainment of emergency jump kits. Jump kits should contain backup spare parts, backup hard copies of key documentation including diagrams, technical manuals, call lists with current contact information, backup licenses and clean copies of software, program logic, logs, and other information on a secure external hard drive. Jump kit should also include any forensics/OT tool kits on removable media.

TASK ID #:	Start Date:	Finish Date:	EST. TIME TO FINISH:	PHASE:
7			12 months	3
ROLES/RESOURCES:		Automation Engineer, IT/CIO, ICS Security Engineer/Manager, IT Security Staff, CISO, Facilities Manager/Construction Project Manager, Physical Security, Contract Management Staff, ICS OEM Vendor, Contractor, Integrator/EPC, ICS Security services firm, Automation Superintendent, Asset Owner VPs		

TASK: Leverage ICS-CERT, US Cyber Command, NSA, SANS ICS, ISA, and NIST standards and recommended BEST practices for ICS/OT incident response. Ensure roles, responsibilities, events, incidents, and points of contact are defined in policies and procedures. Ensure that IT policies and procedures do not conflict with or do harm to ICS/OT specific policies, processes, and procedures. Ensure pre-established contacts with third-parties, ICS-CERT, ICS vendors, MS-ISAC, sector ISAC, and law enforcement exist for each region, brand and ICS asset prior to an incident or event occurring. Ensure policies and procedures create annual exercises and testing windows for each brand and ICS and lessons learned analysis to improve annually. Ensure a chain of command that defines roles and responsibilities between Automation Engineers, Facilities, Physical Security, Safety, HR, IT, IT Security, Automation Superintendent, CIO, CISO and asset owner VPs is well written and practiced on at least a quarterly basis. Ensure internal and external communications plans, methods, tools, and points of contact are established and tested at least quarterly or twice a year. CONSULTANT ICS also has an existing ICS/OT specific IR program guide that we share on projects with our customers to help build ICS specific IR procedures, plans, and policies.

TASK ID #:	Start Date:	Finish Date:	EST. TIME TO FINISH:	PHASE:
8			6 months	2
ROLES/RESOURCES:		Automation Engineer, IT/CIO, ICS Security Engineer/Manager, IT Security Staff, CISO, Facilities Manager/Construction Project Manager, Physical Security, Contract Management Staff, ICS OEM Vendor, Contractor, Integrator/EPC, ICS Security services firm, Automation Superintendent, Asset Owner VPs		

TASK: Create policies and procedures that document and establish clear lines of communication and a very specific chain of command from operations in the field to Automation Superintendent to CISO to CIO to Board. A proper chain of command should be established prior to events and incidents to evaluate and determine an event, escalate to an incident, and elevate up the chain for proper containment, response, eradication, recovery, lessons learned and internal as well as external communications during and after events. Policies and procedures should include authority letters, succession plan in chain of command in case communications is lost as well as authorizations for forensics/OT tools and collaboration with specific qualified personnel (e.g., ICS-CERT). This is specifically important for all ICS/OT assets, assets that will impact the safe operation of the ICS/OT and/or the safety of all personnel.

TASK ID #:	Start Date:	Finish Date:	EST. TIME TO FINISH:	PHASE:
9			24 months	5
ROLES/RESOURCES:		Automation Engineer, IT/CIO, ICS Security Engineer/Manager, IT Security Staff, CISO, Facilities Manager/Construction Project Manager, Physical Security, Contract Management Staff, ICS OEM Vendor, Contractor, Integrator/EPC, ICS Security services firm, Automation Superintendent, Asset Owner VPs		

TASK: Develop policies and procedures for a smart key management system that leverages and deploys the use of custom smart keys to lock cabinets, racks, closets, vehicles, and control boxes that allow physical access to critical equipment. This is especially important for physical access to all communications equipment such as routers, switches, radio and satellite communications modules and ICS/OT assets such as PLC, RTU, HMI, HVAC controllers like JACE and safety devices. The usage of smart locks is not recommended due to Bluetooth, Wi-Fi, Z**IGBEE,** and other RF/wireless attack vectors that enable attacks to compromise smart locks. Smart keys do not depend on such attack vectors and can be easily managed if the keys are lost, stolen, or not returned by an employee or contractor for example. Silent

alarming and monitoring capabilities should be investigated in combination with physical smart key solutions. Such solutions enable time-based access control and record of access to locked areas. Naming conventions for keys can be created by role, department, ICS asset type etc. (e.g., Naming convention for group of contractors on any ICS). This allows for easy disablement of keys or reassignment of keys as needed. This key management program should be implemented for the most critical assets and sites for business operations and safety.

TASK ID #:	Start Date:	Finish Date:	EST. TIME TO FINISH:	PHASE:
10			6 months	2
ROLES/RESOURCES:		Automation Engineer, IT/CIO, ICS Security Engineer/Manager, IT Security Staff, CISO, Facilities Manager/Construction Project Manager, Physical Security, Contract Management Staff, ICS OEM Vendor, Contractor, Integrator/EPC, ICS Security services firm, Automation Superintendent, Asset Owner VPs		

TASK: Create policies and procedures to control the flow of physical access to tank batteries, Wells, SWDs and other critical operational sites. Ensure that all visitors including third parties on contract must check in and sign in with ID at the regional field office. Ensure that third parties also notify you of which personnel they are sending out and require them in all contracts to check in face to face with field offices first prior to going out to a field site and asset. Ensure policies and procedures also include a suspicious and unauthorized visitor reporting process. Ensure the engineers in the field challenge all personnel including third parties that are on site unexpected. Create a reporting chain through the field office up to the Automation Superintendent, Facilities Management, Construction Management, Physical Security, and other areas of Corporate (e.g., IT Security, CISO, CIO, HR etc). Reporting procedure should include date, estimated time, site location, description of vehicle and persons challenged and their stated reason for being at the site unexpectedly or without prior checking in with the local field office. Attackers often leverage social engineering and physical red teaming and reconnaissance tactics, techniques, and procedures to learn as much about their targets as possible prior to or in addition to trying to target ICS assets and operations through other means such as the corporate network, RF/wireless and the internet.

TASK ID #:	Start Date:	Finish Date:	EST. TIME TO FINISH:	PHASE:
11			12 months	3
ROLES/RESOURCES:		Automation Engineer, IT/CIO, ICS Security Engineer/Manager, IT Security Staff, CISO, Facilities Manager/Construction Project Manager, Physical Security, Contract Management Staff, ICS OEM Vendor, Contractor, Integrator/EPC, ICS Security services firm, Automation Superintendent, Asset Owner VPs		

TASK: Ensure technical policies and procedures enforce segmentation and segregation of IT, internet, third-party and ICS assets in the field through a defense-in-depth and breadth approach of DMZs, separate access controlled domains for ICS assets in the field, out-of-band and additional communications interfaces for capturing copies of communications traffic and system logs upstream into a DMZ etc. Enforce dynamic access control lists (DACL), firewall rules, VLAN tagging, NAC and other network control features of Cambium, Netonix, MDS INET, Cisco etc. Ensure third-party and corporate connections for command and or control are routed through controlled jump boxes in the DMZ and leverages access control tools such as Xona Systems, Citrix with RSA tokens etc. Ensure major ICS servers such as Kepware, XSPOC and others that require direct communications down to controllers in the field reside in the DMZ

and all traffic to and from those systems to controllers in the field are monitored by ICS protocol parsing capable tools such as Claroty. Ensure that VLAN hopping attack vector features such as core switches using auto-enabled dynamic trunking protocol (DTP) are disabled. VLANs should use specific tags, one for monitor only traffic and another for command and control traffic, with access port and sticky mac security turned on to prevent systems and devices from communicating across zones.

TASK ID #:	Start Date:	Finish Date:	EST. TIME TO FINISH:	PHASE:
12			12 months	3
ROLES/RESOURCES:		Automation Engineer, IT/CIO, ICS Security Engineer/Manager, IT Security Staff, CISO, Facilities Manager/Construction Project Manager, Physical Security, Contract Management Staff, ICS OEM Vendor, Contractor, Integrator/EPC, ICS Security services firm, Automation Superintendent, Asset Owner VPs		
TASK: Create and disseminate network security policies and procedures that include the enablement of port security, specific VLAN tagging with switch port access control enabled within each VLAN (e.g., mab, 802.1x, sticky mac). Ports should never be enabled to allow anyone to connect to open ports on any switch or network drop. All active ports should have port security rules to prevent unauthorized assets from communicating via active ports that are used on say Netonix, Cambium, Cisco router, or switch, Ntron switch, Freewave radios or any PLC, RTU, HMI, gateway etc.				

TASK ID #:	Start Date:	Finish Date:	EST. TIME TO FINISH:	PHASE:
13			6 months	2
ROLES/RESOURCES:		Automation Engineer, IT/CIO, ICS Security Engineer/Manager, IT Security Staff, CISO, Facilities Manager/Construction Project Manager, Physical Security, Contract Management Staff, ICS OEM Vendor, Contractor, Integrator/EPC, ICS Security services firm, Automation Superintendent, Asset Owner VPs		
TASK: Create policy and procedures to ensure proper vetting and verification for need-to-know access to all ICS/OT assets, information, and field sites. Ensure complete personnel check-in to check-out tools, processes and procedures are implemented for Customer employees as well as third-party support. This should include background checks and collaboration with the ICS Configuration Management Council to determine roles and access requirements with HR, Contracting, IT, Automation, Physical Security, Safety etc. This includes access to documentation such as diagrams that lay out all ICS/OT compartments including the location of electrical closets and areas that would have CCTV, HVAC, fire and life safety, routers and switches and other equipment that can be leveraged as a beachhead attack surface for additional attacks. Ensure field office and corporate office HVAC, chiller, fire, safety, CCTV, and access badge reader systems are also treated as building control and automation systems and operational technology that leverages the same protocols as more industrialized field controllers. The JACE and Lenel devices are perfect examples that are facilities and building related ICS/OT assets.				

TASK ID #:	Start Date:	Finish Date:	EST. TIME TO FINISH:	PHASE:
14			12 months	3

ROLES/RESOURCES:	Automation Engineer, IT/CIO, ICS Security Engineer/Manager, IT Security Staff, CISO, Facilities Manager/Construction Project Manager, Physical Security, Contract Management Staff, ICS OEM Vendor, Contractor, Integrator/EPC, ICS Security services firm, Automation Superintendent, Asset Owner VPs
TASK: Ensure syslog, firewalls, access list, mac filtering, NTP, secure remote access, secure community strings and dynamic and zone unique preshared keys are enabled in all communications devices that are capable such as MDS INET, Netonix, and Cambium devices. Consider replacing the Freewave assets on retrofit projects with radios that have advanced security features such as logging, firewalls, IDS/IPS, additional out-of-band trunks, antijamming, mesh, port security, encryption**,** and authentication features etc such as Ultra3eTi and Motorola radios with advanced features.	

TASK ID #:	Start Date:	Finish Date:	EST. TIME TO FINISH:	PHASE:
15			6 months	2
ROLES/RESOURCES:	Automation Engineer, IT/CIO, ICS Security Engineer/Manager, IT Security Staff, CISO, Facilities Manager/Construction Project Manager, Physical Security, Contract Management Staff, ICS OEM Vendor, Contractor, Integrator/EPC, ICS Security services firm, Automation Superintendent, Asset Owner VPs			
TASK: Work with contracting to audit all existing and pending third-party agreements to insert clauses that enables you to force the removal of all ICS/OT and IoT devices from communicating to the internet directly. Ensure this includes the third parties only connecting remotely to any devices such as PLCs, RTUs, CCTV cameras, badge readers, Fire and HVAC etc through a secure DMZ with a jump server monitored and controlled by Customer 24/7/365. Consider leveraging tools such as Xona Systems to do so. Require the third parties to perform at least a monthly or quarterly test checking tools such as Shodan and internet based scans to provide reporting and alerting if devices managed by third parties show up on the internet. Third party examples to start with should be Integrator/EPC/OEM and Integrator/EPC/OEM.				

TASK ID #:	Start Date:	Finish Date:	EST. TIME TO FINISH:	PHASE:
16			12 months	3
ROLES/RESOURCES:	Automation Engineer, IT/CIO, ICS Security Engineer/Manager, IT Security Staff, CISO, Facilities Manager/Construction Project Manager, Physical Security, Contract Management Staff, ICS OEM Vendor, Contractor, Integrator/EPC, ICS Security services firm, Automation Superintendent, Asset Owner VPs			
TASK: Create maintenance contract to provide upgrades to all outdated equipment that currently has no maintenance or upgrade lifecycle support. Ensure agreements include assets such as moxa switches, Ntron switches, engineering workstations, HMI, PLC, RTU, modems, serial converters such as Digiport etc. Ensure contracts include delivery of and the continuous maintenance of system and device configuration documentation, system security plans, technical manuals, user guides, troubleshooting manuals, fat/sat and commissioning guides and tools, ports,				

protocols, services, registry settings and dependency software or applications. Also ensure agreements include patching and configuration changes as well as compliance with and participation with Customer scheduled at least quarterly maintenance and testing windows.

TASK ID #:	Start Date:	Finish Date:	EST. TIME TO FINISH:	PHASE:
17			18 months	4
ROLES/RESOURCES:		Automation Engineer, IT/CIO, ICS Security Engineer/Manager, IT Security Staff, CISO, Facilities Manager/Construction Project Manager, Physical Security, Contract Management Staff, ICS OEM Vendor, Contractor, Integrator/EPC, ICS Security services firm, Automation Superintendent, Asset Owner VPs		

TASK: Investigate, test, consider and deploy implementation of RADIUS, TACACS and separate active directory domains between DMZ, ICS security stack, ICS networks**,** and corporate network. Ensure zero trust between zones and across DMZ. Where assets are capable of support RADIUS, TACACS and similar security features then implement in a phased approach zone by zone. An example of a zone would be a grouping of wells that have a need to speak to each other in the same regions or wells and tank batteries within a region that speak to each other for operational regions. Consider the creation of sub zones that segregate tank batteries by regions, wells by regions, SWDs by regions etc. Use RADIUS, TACACS, active directory, access control rules, VLANs, industrial firewalls etc to control protocol and communication flow between these sub zones. This should include leveraging tools like Xona Systems to control third-party access to assets in each zone through a jump box in the DMZ.

TASK ID #:	Start Date:	Finish Date:	EST. TIME TO FINISH:	PHASE:
18			18 months	4
ROLES/RESOURCES:		Automation Engineer, IT/CIO, ICS Security Engineer/Manager, IT Security Staff, CISO, Facilities Manager/Construction Project Manager, Physical Security, Contract Management Staff, ICS OEM Vendor, Contractor, Integrator/EPC, ICS Security services firm, Automation Superintendent, Asset Owner VPs		

TASK: Create project to implement security gateways, zones, firewalls, IDS/IPS and monitoring solutions for Freewave devices. No Security zones, monitoring or firewalls appeared to exist. No confirmation that Freewave can defend or detect against man-in-the-middle attacks, network, device, software**,** or protocol-based attacks. No confirmation of any logging features that would allow monitoring for such attacks on or from other interconnected ICS/OT systems. We recommend replacing these with more secure (i.e.**,** Cambium) devices or adding an industrial firewall device capable of securing the transmission to mitigate this potential attack vector such as Siemens Scalance S, Phoenix Contact MGuard and Belden Tofino Xenon.

TASK ID #:	Start Date:	Finish Date:	EST. TIME TO FINISH:	PHASE:
19			12 months	3
ROLES/RESOURCES:		Automation Engineer, IT/CIO, ICS Security Engineer/Manager, IT Security Staff, CISO, Facilities Manager/Construction Project Manager, Physical Security, Contract Management Staff, ICS OEM Vendor, Contractor, Integrator/EPC, ICS Security services firm, Automation Superintendent,		

	Asset Owner VPs
TASK: Create policy and procedure that ensures all CD/DVD, USB, external drives, and other input media devices are restricted to Customer owned devices that are regularly hardened, scanned, tested through malware sandboxes, and remain under a strict chain of custody at all field offices as well as corporate. Ensure only the authorized inventory of controlled and tagged devices are used to connect to controllers, engineering workstations, laptops, and tablets used to make changes to devices in the field including communications devices.	

TASK ID #:	Start Date:	Finish Date:	EST. TIME TO FINISH:	PHASE:
20			18 months	4
ROLES/RESOURCES:		Automation Engineer, IT/CIO, ICS Security Engineer/Manager, IT Security Staff, CISO, Facilities Manager/Construction Project Manager, Physical Security, Contract Management Staff, ICS OEM Vendor, Contractor, Integrator/EPC, ICS Security services firm, Automation Superintendent, Asset Owner VPs		
TASK: Create Factory Acceptance Test (FAT), Site Acceptance Test (SAT) and Commissioning guides, procedures and technical requirements for all brownfield retrofits and all new greenfield projects. Require in all contracts that all third parties provide this documentation to the Automation Engineers, Automation Superintendent, Facilities, Physical Security, Safety, IT Security and Construction Management. Ensure this information is shared with the CCB so that Contracting and other parties within the company with a potential need for awareness to support operations related needs and contract agreements have visibility. FAT, SAT, and Commissioning should include documented details of process logic design, purpose, steps, expected configurations and outcomes, updated engineering drawings including of the network communications, registers, set points, protocols used (especially ICS protocols). The documents should be written in such a way that all engineers including engineers who may not have been on a project can pick up the documents and run through an end user acceptance test or system validation test to verify the assets are designed, operating and configured as documented and expected in FAT, SAT and Commissioning. Additionally, an independent third-party ICS security firm should perform a security FAT, security SAT, and security checks during Commissioning to look for weaknesses and vulnerabilities in system design, system configuration, program logic in PLCs, RTUs, applications, implementation of best security practices on controllers, communication devices, HMIs, workstations, servers etc. This third-party independent firm should have ICS security experiences and provide a security FAT/SAT procedure that details the kinds of testing and tools to be used with a copy of the data collected and analyzed and a list of recommendations to include a tracking list of which assets were tested, by whom, when, how and with which tools etc. Example third parties to begin enforcing this in contracts with is Tank Logix, Remote Monitoring Services, Deans etc.				

TASK ID #:	Start Date:	Finish Date:	EST. TIME TO FINISH:	PHASE:
21			12 months	3
ROLES/RESOURCES:		Automation Engineer, IT/CIO, ICS Security Engineer/Manager, IT Security Staff, CISO, Facilities Manager/Construction Project Manager, Physical Security, Contract Management Staff, ICS OEM Vendor, Contractor, Integrator/EPC, ICS Security services firm, Automation Superintendent, Asset Owner VPs		

TASK: Ensure that an independent ICS security experienced group of experts perform annual assessments, penetration tests, POA&M reviews and updates, risk modeling and other services that require regular support. This support is in addition to at least annual self-assessments and exercises that Customer should perform for itself with all stakeholders involved such as Physical Security, Safety, IT Security, Facilities, Automation and Construction. Ensure lessons learned are regularly shared with both the CCB and the ICS security council to ensure that lessons learned help executives drive needed changes in business practices and contractual agreements with third parties.

TASK ID #:	Start Date:	Finish Date:	EST. TIME TO FINISH:	PHASE:
22			12 months	3
ROLES/RESOURCES:		Automation Engineer, IT/CIO, ICS Security Engineer/Manager, IT Security Staff, CISO, Facilities Manager/Construction Project Manager, Physical Security, Contract Management Staff, ICS OEM Vendor, Contractor, Integrator/EPC, ICS Security services firm, Automation Superintendent, Asset Owner VPs		

TASK: Ensure all applications implement multifactor authentication. This is especially important for cloud to mobile app solutions. Leverage tools such as Xona systems where both third parties and Customer employees require app and remote access to ICS/OT assets in the field. This enables ease of access control management with unique login tracking for each user. This also improves session control, session logging, time based access for changes (especially with third parties) etc.

TASK ID #:	?:	?:	EST. TIME TO FINISH:	PHASE:
23			90 days	1
ROLES/RESOURCES:		Automation Engineer, IT/CIO, ICS Security Engineer/Manager, IT Security Staff, CISO, Facilities Manager/Construction Project Manager, Physical Security, Contract Management Staff, ICS OEM Vendor, Contractor, Integrator/EPC, ICS Security services firm, Automation Superintendent, Asset Owner VPs		

TASK: Create policies, procedures, memos, directives and orders the enterprise clearly defining roles, responsibilities and authorities for configuration, administration, access control, management, maintenance and implementation of ICS/OT security technical configurations, monitoring, analysis, operations and approval and tracking of systems security engineering integration into ICS/OT assets and engineering projects. Specifically define the ICS/OT role of both Automation and IT staff with a focus of enabling Automation staff to operate in isolation mode if timely support and communications from corporate or third parties is not feasible or risk appropriate to maintain secure and safe operations of critical ICS/OT systems.

TASK ID #:	Start Date:	Finish Date:	EST. TIME TO FINISH:	PHASE:
24			12 months	3
ROLES/RESOURCES:		Automation Engineer, IT/CIO, ICS Security Engineer/Manager, IT Security Staff, CISO, Facilities Manager/Construction Project Manager, Physical		

	Security, Contract Management Staff, ICS OEM Vendor, Contractor, Integrator/EPC, ICS Security services firm, Automation Superintendent, Asset Owner VPs

TASK: Create procedures, test and development lab and policies for regular maintenance windows at least quarterly for all critical ICS/OT assets, systems**,** and networks. Divide the lifecycle up by zones (e.g.**,** Wells in different regions, Tank batteries in different regions etc) to ensure that system patching and major system changes and updates do not create widespread operational degradation or outages. These maintenance windows should define patching and vulnerability scanning schedules for each zone and type of systems (e.g.**,** zone X for Wells and system type or brand Y). Ensure test and development lab leverages and maintains an inventory of spare parts and mimics/OT production environments for various types of sites and brands used in the field.

TASK ID #:	Start Date:	Finish Date:	EST. TIME TO FINISH:	PHASE:
25			6 months	2
ROLES/RESOURCES:		Automation Engineer, IT/CIO, ICS Security Engineer/Manager, IT Security Staff, CISO, Facilities Manager/Construction Project Manager, Physical Security, Contract Management Staff, ICS OEM Vendor, Contractor, Integrator/EPC, ICS Security services firm, Automation Superintendent, Asset Owner VPs		

TASK: Define tool and technology requirements and procure solutions that can be used to track, risk rate, report upon and improve the key performance indicators and risk metrics/OT of the ICS/OT cyber security management system/program. (e.g.**,** tools that leverage the best of breed approach from models such as FAIR, FMEA, OCTAVE, TARA, Bowtie etc like Risk Lens)

TASK ID #:	Start Date:	Finish Date:	EST. TIME TO FINISH:	PHASE:
26			90 days	1
ROLES/RESOURCES:		Automation Engineer, IT/CIO, ICS Security Engineer/Manager, IT Security Staff, CISO, Facilities Manager/Construction Project Manager, Physical Security, Contract Management Staff, ICS OEM Vendor, Contractor, Integrator/EPC, ICS Security services firm, Automation Superintendent, Asset Owner VPs		

TASK: Create and or contract an independent team of ICS/OT security technical expert penetration testers, system security engineer testers and validators that report their findings to the responsible/supported ICS/OT security roles and the designated ICS/OT security program manager and authorizing official who owns the ICS/OT assets. These roles should be filled by the asset owners, the Automation Superintendent and the supporting CISO, IT Security Director/Manager who has ICS experience or a team of contracted ICS Security Managers as a Service. This provides regular independent**,** and ICS experienced eyes on all ICS assets and operations to ensure the roadmap tasks are continuously implemented and maintained throughout the lifecycle of ICS assets.

TASK ID #:	Start Date:	Finish Date:	EST. TIME TO FINISH:	PHASE:
27			12 months	3
ROLES/RESOURCES:		Automation Engineer, IT/CIO, ICS Security Engineer/Manager, IT Security Staff, CISO, Facilities Manager/Construction Project Manager, Physical Security, Contract Management Staff, ICS OEM Vendor, Contractor, Integrator/EPC, ICS Security services firm, Automation Superintendent, Asset Owner VPs		
TASK: Have the ICS/OT Security Program Manager create policies, procedures and schedules for mandatory annual operational security and safety exercises that test incident response and business continuity against real-time penetration testers and vulnerability assessments. This should be scheduled through the ICS Configuration Council and the CCB. These exercises should be used to practice and improve policies, procedures, personnel, business processes, ICS assets and supporting infrastructure.				

TASK ID #:	Start Date:	Finish Date:	EST. TIME TO FINISH:	PHASE:
28			6 months	2
ROLES/RESOURCES:		Automation Engineer, IT/CIO, ICS Security Engineer/Manager, IT Security Staff, CISO, Facilities Manager/Construction Project Manager, Physical Security, Contract Management Staff, ICS OEM Vendor, Contractor, Integrator/EPC, ICS Security services firm, Automation Superintendent, Asset Owner VPs		
TASK: Create and announce task leads for each of the various tasks within this roadmap POA&M. The task leads will be responsible to the Council and the CCB monthly for providing progress updates, raising of issues, offering solutions to issues, requesting resources etc.				

TASK ID #:	Start Date:	Finish Date:	EST. TIME TO FINISH:	PHASE:
29			12 months	3
ROLES/RESOURCES:		Automation Engineer, IT/CIO, ICS Security Engineer/Manager, IT Security Staff, CISO, Facilities Manager/Construction Project Manager, Physical Security, Contract Management Staff, ICS OEM Vendor, Contractor, Integrator/EPC, ICS Security services firm, Automation Superintendent, Asset Owner VPs		
TASK: Create roles, responsibilities, access control and technical procedures and tools for remote access monitoring and control of ICS/OT assets. Ensure all contracts, supported and supporting roles clearly define when, where, how and for what reason remote access to ICS/OT should occur. Ensure all access is time limited. For example, a lesson learned from the Ukraine power grid hack through trusted VPN connections is to never allow persistent, always-on remote connections to ICS/OT assets, including the engineering workstations and human machine interface (HMI) terminals or tablets. It is best to only allow access upon special request as needed to perform remote ICS/OT				

functions. All remote access sessions and accounts both technology and human-based accounts should be monitored and time controlled. Monitoring should include industrial protocol monitoring for unauthorized, unexpected, abnormal**,** or unscheduled commands going to and from ICS/OT assets.

Appendix 2: List of Required Recommended ICS/OT Security Trainings and Roles

At least one of the trainings should be initially required with the remaining trainings being used for at minimum annual continuous training in ICS/OT specific security standards, tactics/OT, techniques, procedures, best practices, tools, technologies, threats, vulnerabilities, risks, and current events. Passing of certificate and certification exams is not required, but for key roles it is very strongly recommended. Proof of course completion, however, in all cases is mandatory and should be tracked from the ICS to shore to corporate security levels of the enterprise.

Training Name	Organization	Role	Requirement	References
ISA 62443 INDUSTRIAL CYBERSECURITY CERTIFICATE PROGRAM (1 - 4) trainings	International Society of Automation (ISA)	ICS Security Officer, Electro-Technical Officer, IT Officer, Shore and Corporate Security supporting roles, ICS/OT contractor, integrator & vendors	Required; other roles optional and encouraged	https://www.isa.org/certification/certificate-programs/isa-iec-62443-cybersecurity-certificate-program
SANS ICS ICS410: ICS/SCADA Security Essentials - GICSP Certification possible	SANS Institute	ICS Security Officer, Electro-Technical Officer, IT Officer, Shore and Corporate Security supporting roles, ICS/OT contractor, integrator & vendors	Required; other roles optional and encouraged	https://www.sans.org/cyber-security-courses/ics-scada-cyber-security-essentials
SANS ICS ICS515: GRID certification possible	SANS Institute	ICS Security Officer, Electro-Technical Officer, IT Officer, Shore and Corporate Security supporting roles, ICS/OT contractor, integrator & vendors	Required; other roles optional and encouraged	https://www.sans.org/cyber-security-courses/ics-visibility-detection-response

SANS ICS 612: Defense-in-Depth	SANS Institute	ICS Security Officer, Electro-Technical Officer, IT Officer, Shore and Corporate Security supporting roles, ICS/OT contractor, integrator & vendors	Required; other roles optional and encouraged	https://www.sans.org/cyber-security-courses/ics-cyber-security-in-depth
ICS-CERT Virtual Learning web ICS/OT intro courses	DHS ICS-CERT	Global Security Director, CISO, Admiral, Captain, ICS/OT Project Management/Engineers, ICS/OT procurement and contracting, CIO and communications staff, applicable contractors, vendors, and integrators	Required; other roles optional and encouraged	https://www.cisa.gov/resources-tools/programs/ics-training-available-through-cisa
ICS-CERT VIRTUAL LEARNING WEB ICS/OT INTRO COURSES	DHS ICS-CERT	ICS security officer, electro-technical officer, IT officer, shore and corporate security supporting roles, ICS/OT contractor, integrator & vendors	Optional if more advanced trainings from sans, isa etc. have been completed, if not then required in addition to more Advanced trainings	https://www.cisa.gov/resources-tools/programs/ics-training-available-through-cisa

Appendix 3: Roles & Responsibilities for ICS/OT Security

Below is a recommended table of responsible or supported roles for ICS/OT security and supporting roles for ICS/OT security. The "supported" responsible role is primarily responsible for ensuring, enforcing, tracking, creating, tracking, monitoring, implementing, reporting, and maintaining security best practices, policies, procedures, guidelines, directives, orders, standards and regulation requirements for ICS/OT assets and connections to ICS/OT (e.g., from a vendor, integrator, contractor). The "supporting" roles are responsible for ensuring that all their services, infrastructure, assets, and operations do no harm to the security and safety of ICS/OT assets and operations. The supporting roles are to provide all support, services and equipment needed and or requested from the supported responsible roles.

Roles	Responsible/(Supported)/ Supporting	Duty
Automation Engineer	Responsible	ICS/OT Security
IT/CIO	Supporting	ICS/OT Security support
ICS Security Engineer/Manager	Responsible	ICS/OT Security

IT Security Staff	Supporting	ICS/OT Security Support
CISO	Supporting	ICS/OT Security Support
Facilities Manager/Construction Project Manager	Responsible	ICS/OT Security
Physical Security	Supporting	ICS/OT Security Support
Contract Management Staff	Supporting	ICS/OT Security Support
ICS OEM Vendor	Responsible	ICS/OT Security
Contractor	Responsible	ICS/OT Security
Integrator/EPC	Responsible	ICS/OT Security
ICS Security services firm	Supporting	ICS/OT Security Support
Automation Superintendent	Responsible	ICS/OT Security
ASSET OWNER VP	Responsible	ICS/OT Security