American Public Gas Association

Security Self-Assessment Tool – Submitter's Guide

EVERLINE ENERGY'S TECHNICAL STACK

Message from APGA

Dave Schryver, APGA President & CEO

At APGA, safely and securely delivering natural gas to customers is our members' highest priority. As cybersecurity threats continue to grow in both complexity and frequency, it is essential that every public gas system take proactive steps to better protect their infrastructure. To guide our members in this effort, APGA has developed a cybersecurity hygiene assessment tool tailored specifically for public natural gas systems. This tool is designed to help you evaluate your current cybersecurity practices, identify potential gaps, and strengthen your overall security posture. I strongly encourage all members to use this resource as part of your ongoing commitment to operational resilience and the continued protection of the communities you proudly serve. By staying vigilant and prepared, our members can continue to safely deliver reliable energy to their customers.

Message from EverLine

Mike Bradley, EverLine Utilities Director

APGA members are the bedrock of safe, reliable, affordable energy delivery across America's vast geography and EverLine appreciates the opportunity to leverage our experience and expertise in energy infrastructure security in developing training and resources for this incredible organization and its members.

Thank you for taking the time to complete the Self-Assessment, which we hope will be both educational and informative as the topic of infrastructure security continues to increase in both prevalence and priority amongst the numerous responsibilities of operations leaders.

Please be verbose with your feedback on the assessment tool, this guide, and the process in general; our goal is to provide you with up-to-date tools that allow you to stay ahead of both the threat and regulatory environments and we are committed to continuous improvement.

What is the Security Self-Assessment Tool?

The Security Self-Assessment Tool was created by APGA and EverLine with two goals in mind:

1. Develop a guide for public utility operators to meaningfully engage in the concepts and vernacular of operational technology (OT) cybersecurity.
2. Provide a no-cost, first-step method for assessing their cybersecurity posture.

This tool is designed as a voluntary, self-guided assessment akin to tools previously developed for APGA.

While the universe of cybersecurity assessment, preparation, monitoring, response, recovery, and investigation are vast and technical, this APGA Security Self-Assessment Tool has been designed to capture high-level elements.

The tool utilizes a modified maturity model scoring system with points assigned from 0 to 4 across each question. At the completion of the assessment, a score will be provided out of the total.

The scores generated in this tool will be used for aggregated analysis and trending by APGA. APGA will only use aggregated and/or non-attributed scores in communications with internal or external audiences.

This self-assessment is meant to be used as a guidance and benchmarking tool ONLY and is NOT intended and CANNOT be used to ensure compliance with applicable cybersecurity laws and regulations.

Why should I use this tool?

This tool is intended for use by individuals at your system who are accountable for the security and safety of your natural gas pipeline systems. It is designed to aid in self-assessment of your system's preparedness for cybersecurity incidents and response.

Cyber-attacks on American infrastructure continue to rise annually. Additionally, federal regulators, legislators, and the insurance community have heightened interest in energy security. This tool is designed to help public gas utilities be better prepared, which is critical in the prevention of safety-sensitive and/or financially damaging incidents.

What type of information will I provide in this tool?

The questions and answers in this tool, while relevant to security topics, do not comprise Sensitive Security Information (SSI), as defined by Transportation Safety Administration (TSA). Responses to this tool are most closely associated with Internal information, although your own security plan may classify it differently. Please refer to your Information Classification Plan (if available) to verify prior to using this tool.

Furthermore, the tool only collects general demographic data to be retained in the database as well as your APGA Member ID, which is only available to you and APGA staff. This identifier is not accessible to EverLine.

At no time are personnel names, contact information, operator names, or other publicly identifiable information collected by the tool or correlated in the collected data.

How will my information be used and by who?

APGA may utilize the aggregated and/or non-attributed data collected from this tool in support of its federal regulatory and legislative advocacy.

The insights from the results of this tool may also help inform APGA and EverLine's efforts to develop further resources to aid APGA members in assessing their implementation of cybersecurity best practices.

What is this document?

This document is designed as a guide for those completing the Self-Assessment. It offers basic considerations as well as question-specific information to educate the user and provide context for the questions in the assessment.

We recommend having this document available to you as you complete the questionnaire.

Self-Assessment General Tips

- Use "unsure" answers sparingly.
    - We encourage submitters to seek answers from within their organization in the event that elements are in place but not widely communicated.
    - The "unsure/don't have" options are synonymous and carry a maturity score of 0. This is because in the event of an incident, neither scenario will be helpful in safeguarding your system.
- If you would like additional information or assistance with this tool, please submit an email to APGASecurityTool@Everlineus.com.
- Since the tool is anonymous, the submitter cannot save progress and return later, the survey must be completed in one browser session.
    - It is recommended that the submitter use the Submitter's Guide to prepare answers in advance, then use the live tool for only for submittal of responses.
- There is no administrative control to prevent multiple submittals from one Operator; recommend coordinating response internally.

REMINDER: Never include sensitive information in any correspondence.

Who is EverLine?

EverLine is an active APGA Associate Member that specializes in OT cyber and physical security, remote operations, SCADA, and managed OT networks for energy infrastructure operators in the U.S.

While we are a vendor, we are also an operator. EverLine operates the largest third-party control room for pipeline assets in North America and operates assets ranging from gathering and production through midstream, transmission, and distribution systems.

While our client base ranges from industrial end-users to majors, as well as both investor-owned and municipal utilities, many of our clients are small-midsize and our collective lived experiences echo those of APGA members.

Definitions

Attack Surface means the sum of all possible points where an unauthorized user can try to enter data into or extract data from an environment. This includes all the hardware, software, and network components that could be exploited by an attacker.

Cybersecurity means the practice of protecting networks, devices, and data from unauthorized access or criminal use. It involves implementing technologies, processes, and policies to safeguard computer systems, applications, data, and financial assets from cyber threats such as malware, phishing, and data breaches.

Data (in this context) refers to information in digital form that is created, or utilized, by asset owners in operational and business environments.

DMZ (Demilitarized Zone) is a segmented network area that acts as a buffer between an organization's internal network and untrusted external networks (like the internet).

Logging means the systematic recording of events, activities, and messages generated by network devices, servers, and applications.

Risk means the potential for loss or harm related to technical infrastructure, use of technology, or reputation of an organization. It involves the likelihood of a cyberattack or data breach and the potential consequences, such as financial loss, reputational damage, or operational disruption.

SSI means sensitive security information as described in 49 CFR 1520.5, specifically 1520.5(a)(3): "information…the disclosure of which TSA has determined would be detrimental to the security of transportation."

Supply Chain is the structure of goods and services provided to deliver energy to the broader public.

Threat means any circumstance or event with the potential to adversely impact organizational operations, assets, individuals, or the nation through unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

TSA means the Transportation Security Administration.

Vendor is a term used to describe an entity that provides goods or services to an asset owner. Some vendors may be considered a critical part of the supply chain.

References

The universe of security requirements and best practices is vast, with numerous standards available from government and non-government sources. Unlike pipeline safety regulations as found in 49 CFR 190-199, most security practices are not required* for non-critical pipeline operators as of the time of this publication.

- Code of Federal Regulations, 49 CFR Part 1520 Sensitive Security Information**
- TSA Security Directive Enhancing Pipeline Cybersecurity 2021-01
- TSA Security Directive Enhancing Pipeline Cybersecurity 2021-02E
- TSA 2018 Pipeline Cybersecurity Guidelines + April 2021 Change*
- TSA Information Circular (IC) to Enhance Pipeline Cyber Security (IC Pipeline-2022-02)**
- API 1164v3 Pipeline Control Systems Cybersecurity**
- IEC/ISA 62443 Series**
- NIST 800-82 Guide to Operational Technology Security**
- NIST 800-53 Security and Privacy Controls for Information Systems and Organizations
- NIST 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
- NIST Cybersecurity Framework**
- NVIC 01-20 Guidelines for Addressing Cyber Risks at MTSA Regulated Facilities
- USCG 2022-0802 Cybersecurity in the Marine Transportation System
- NERC Critical Infrastructure Protection (CIP)
- FERC Order 850
- Relevant State or Commonwealth energy security rules, regulations, or guidelines

*Some are strongly recommended or may be required by your insurance, and others may become mandatory in future rulemakings

**Denotes greater likelihood of applicability to APGA member operators

Legal Disclaimer

The APGA Security Self-Assessment Tool and Submitters Guide (collectively, the "tool"), developed in partnership with Everline, is intended to enhance APGA system member awareness of cybersecurity practices and current implementation within their system. The tool provides general information that is intended, but not guaranteed, to be correct and up-to-date. APGA and EverLine will make an effort to promptly correct errors in the tool brought to our attention.

The information is not presented as a source of legal or other professional advice. Furthermore, the information provided in the tool should not be used for determining compliance with applicable laws and regulations, as utilization of the tool does not, and is not intended to, guarantee compliance with said laws and regulations. The tool is not a substitute for professional and legal advice on how to comply with applicable laws and regulations. You should consult your compliance officer (or equivalent), attorney, or other knowledgeable professional for legal, compliance, or other advice.

This tool is not intended to collect confidential, proprietary, or security sensitive information. Neither APGA nor EverLine can be held responsible for information inappropriately reported in the tool.

To the full extent permissible by law, APGA and EverLine disclaim all warranties, express or implied. Neither APGA nor EverLine shall be liable for any damages, whether tangible or intangible, arising from the use of or inability to use this tool or any material contained in it, or from any action, including non-actions, or decision taken as a result of using the tool. No one and no entity shall be entitled to a claim for detrimental reliance on any information provided or expressed within the tool.

Question 1:

Q: Does your organization have an Information Classification plan that provides details on how to handle sensitive information?

What is an Information Classification Plan?

An Information Classification Plan is a structured approach to categorizing data based on its sensitivity and the level of protection it requires. Organizations can more effectively manage and protect data by assigning different levels of security controls to different types of data. Resources can be prioritized to the most sensitive data.

Why is it important to have an Information Classification Plan?

Some standards and regulations require organizations to implement data classification to ensure that access controls, encryption, and other safeguards are properly applied to sensitive data.

What are some examples of data categories?

In order from least to most sensitive, and thus least to most secure:

- **Public Data:** Information that is freely available to the public, such as PHMSA Annual Report data containing miles of pipe, numbers of services, number of leaks repaired, etc.
- **Internal Data:** Data used for internal purposes, such as org charts, memos, employee notifications, company policies, etc.
- **Confidential Data:** Data that, if released outside of the authorized users, may create an impact. Such data may be financial records, business plans, inter-employee communications, etc.
- **Restricted Data:** Information that must be protected to comply with legal and regulatory requirements such as HIPAA. This may include personal identifiable information (PII).
- **Critical Data:** Data that is essential to the operation of the organization such as business continuity, disaster recovery, and critical infrastructure information.

References

- TSA Pipeline Security Guidelines (April 2021) – Protect - Data Security & Information Protection baseline requirement.
- NIST Framework

Question 2:

Q: Does your organization have an Incident Response Plan or Disaster Recovery Plan that addresses security incidents?

What is an Incident Response Plan?

An Incident Response Plan is a structured approach for managing and mitigating security incidents including cyber-attacks, data breaches, and the actions of malicious insiders. The goal is a swift and effective response to minimize the impact of such events. Roles, responsibilities, and strategies based on incident type are typically contained in an Incident Response Plan.

What is a Disaster Recovery Plan?

A disaster recovery plan is a structured approach to returning operations to 'normal' as quickly as feasible following an incident. Disaster recovery plans generally contain risk assessments, business impact analysis, recovery strategies, and other relevant topics such as data storage and management, training, and testing of persons and systems.

Is this similar to my Emergency Response Plan (ERP) as required by 49 CFR 192.615?

Yes and No. Since the Colonial Pipeline incident in May of 2021, there has been a push by PHMSA to understand how operators will continue to operate their systems safety in the event of a cyber-attack and there may be operational steps taken on the pipeline system in response to such events; however, pipeline ERPs are generally limited in scope to those activities required by federal and state pipeline safety regulations and do not generally cover the breath of non-operational aspects of cyber incident response.

Why is it important to have an Incident Response Plan and/or Disaster Recovery Plan?

Some standards and regulations require organizations to implement data classification to ensure that access controls, encryption, and other safeguards are properly applied to sensitive data.

References

- TSA Pipeline Security Guidelines (April 2021) – Respond - Response Planning - baseline requirements.
- NIST Framework

Question 3:

Q: Does your organization have a Supply Chain or Vendor Security policy that provides guidance to ensure products and services procured meet your security requirements?

What do my supply chain or vendors have to do with my cyber security?

Often, an operator's contractors, vendors, customers, and suppliers share information and/or processes with the operator. Having visibility over, and managing, how your partners access, store, and use data related to your operations and customers is critical in understanding whether such data is adequately protected and what impact your operations may experience if a partner were to experience an incident.

How does one manage supply chain security?

Knowing what information is, and should be, shared with vendors (hint: Information Classification Plan), and how that information will be transmitted, used, and stored is a must when evaluating supply chain security. There are frameworks (like SOC 2 from the American Institute of Certified Public Accountants) that allow vendors to demonstrate effective controls for data security. Periodically, operators should be assessing their supply chain and validating that controls are in place to protect data.

A note on "cloud" services and applications

In today's day and age, many operators leverage services provided "in the cloud," which simply means using someone else's computers. The "cloud" is not itself a distinct or homogenous entity and there are significant differences amongst cloud services that collect, process, and store operator data; your security controls should be tailored to each.

Question 4:

Q: Does your organization have documented technical security requirements that govern security of networks, systems, and accounts? This should include password requirements, system patching, etc.

Why should we document (and follow) such requirements?

In addition to having strong security practices in place, the requirements, configuration, and implementation expectations should be documented for consistency, auditability, and communication to key stakeholders. Documented practices ensure organizational policies are clearly conveyed to those working in the operational environment. They establish a clear metric on acceptable behaviors and operating within the bounds of corporate priorities, such as safety. Documented policies are important in daily operations but also indicate risk mitigations in place for regulators and insurers. Having documented requirements also makes it easier to evaluate new facilities, services, and vendor connections.

Once the requirements are documented, they should be implemented where applicable through training, administrative and engineered controls, roles and responsibilities and functional processes to ensure adherence.

Question 5:

Q: In your organization, are clear roles and responsibilities established for managing cyber security, physical security, and handling incidents?

Why should roles be defined?

Cyber security is an element in the foundation of safe and stable operations. While all employees have a role in the security of daily operations, ownership of core processes and risk decisions should be assigned as a responsibility of selected employees. These roles are essential to ensuring the organization's risk portfolio is maintained, they serve critical roles in responding to and recovering from incidents, and they can be important points of contact for security matters for all employees.

Question 6:

Q: Does your organization have, and follow, a written policy on logging and monitoring?

Why is logging and monitoring important, and why should it be documented?

Logging and monitoring are technical measures used to provide situational awareness. Without these tools, asset owners would not know if they had anomalous operations or are experiencing a cyber-attack. Early notification can be essential to responding and recovering without operational incident. Like technical security policies, written logging and monitoring policies establish the organization's acceptable situational awareness and provide operational guidelines.

Question 7:

Q: Does your organization have, and follow, a written Security Incident Management Plan?

What is a Security Incident Management Plan and why should it be documented?

Documenting clear processes and procedures to execute during times of crisis can ensure successful, safe response and recovery. A Security Incident Management Plan establishes these processes and identifies clear roles and responsibilities. This Plan serves as a guide for all employees involved in operational incident response.

Question 8:

Q: Does your organization have, and follow, a written Policy for sensitive information handling?

What is sensitive information handling and why should it be documented?

Cyber security does not result solely from technical or digital risks. Information about operations, systems, and networks can provide adversaries with useful data that can be used to exploit the organization and is considered sensitive. Sensitive information should have clearly documented handling guidelines. This includes labeling, storage, transmission, and destruction. This document provides guidance to all employees with access to sensitive information.

Question 9:

Q: Does your organization have a separate OT network for operational, SCADA, and field systems? Or do these systems reside on a single IT network?

What is network separation and why is it important?

Separating operational activities from business activities adds defense-in-depth and additional security measures to the most critical operational processes. When successfully separated at a network level, often using a DMZ, these OT assets are well protected from Internet-based cyber threats. After the Colonial Pipeline incident, the federal government and standards organizations emphasized existing recommendations and added new requirements around network separation of IT and OT assets.

Question 10:

Q: Does your organization utilize the Purdue Enterprise Reference Architecture, "the Purdue Model," to separate IT and OT?

What is the Purdue Model?

The Purdue Enterprise Reference Architecture, or "Purdue Model," is a framework for operational architectures that was developed in the 1990s. This framework defines operations that occur at Levels and provides a mechanism to define layered security and data transfer among the levels. It also provides a common language between asset owners and vendors as they design and implement full operational architecture. Due to its success, the concepts were adopted in the IEC 62443, a global operating standard, that takes the same defense in depth concept and defines in terms of "security zones" and "conduits." This model is the accepted, gold standard for applying security in operational environments.

Question 11:

Q: Does your organization use Multi Factor Authentication (MFA)?

What is Multi-Factor Authentication?

Multi-Factor Authentication, or MFA, is a method that utilizes more than one attribute to grant a user's access to a system or network. MFA examples include a password *and* one of the following: Microsoft Authenticator code, token, and text or voice code via phone. The use of MFA greatly reduces an adversary's chance of exploiting an account and gaining access.

Question 12:

Q: Does your organization have an intrusion detection or monitoring system?

What is an Intrusion Detection System or monitoring system?

An Intrusion Detection System, or IDS, monitors the network for evidence of unauthorized access by an adversary. Some simple IDSs are included in firewall technology. Other systems are more complex and use AI-based monitoring for anomalies across the environment. Monitoring for intrusions provides an immediate alert and, depending on the technology, may also block an adversary's attempt.

Question 13:

Q: Do shared accounts exist on your OT systems? Or does each user have an individual login?

What is a shared account?

When an account username and password are shared among more than one individual, it is considered a shared account. Historically, this process was common with field assets, where multiple field technicians or contractors may need access, especially administrative level access, to systems. Sharing login information creates risks and prevents clear forensics and accountability for specific actions taken by the user. Shared accounts are not recommended.

Question 14:

Q: Do added security controls exist to protect your OT critical systems, such as additional firewalls and reduced, role-based access?

Why are these added controls important?

Unlike IT systems, OT systems, when exploited, can create safety consequences. Exploitation of these systems can create a physical consequence that impacts operations, employees, and the general public. Therefore, OT systems are considered a higher criticality than IT and are protected as such. These extra measures include perimeter protections, like additional firewalls, significant access controls, etc. These added protections create the defense-in-depth that is referenced throughout regulations, standards, and guidelines.

Question 15:

Q: Can you remotely access your OT networks?

What is remote access and why is it important?

Remote access means a user may access a system without physically using a system or access point on the network. Remote access into OT systems can generate risk, as this access provides remote connectivity that could be exploited by an external adversary. Careful configuration is required, with the implementation of security controls, to ensure this access is not used as a vector by an adversary.

Question 16:

Q: Do data security mechanisms exist in your operation that provide for secure transit and storage of sensitive information?

What are data security mechanisms that can provide secure transit and storage of information?

Storing sensitive information on personal computers, in shared digital workspaces, or transmitting via email can provide adversaries with opportunities to intercept and access this information. It also increases the chance of disclosure to an unauthorized individual, even an insider. To protect this information, mechanisms like secure file transfer, file encryption, secure file containers, and online storage with role-based access controls are utilized to prevent unauthorized access.

Question 17:

Q: Does your organization implement physical security?

What is physical security?

Physical security includes protection of assets, sites, and employees at a geographic location. Physical security measures include fencing and perimeter controls, security lighting, surveillance, ingress/egress badge controls, and intrusion detection. Physical security measures can include personnel measures as well as background checks and security training.

Question 18:

Q: Is an identified person or team responsible for managing and conveying threat information?

What is threat information?

Threat information includes details around active adversaries, their tactics, ongoing campaigns, and known or predicted risks to asset owners. This information may include alerts on exploitable vulnerabilities, recommendations for mitigations, and trend analysis. It is collected and disseminated by the federal government, research labs, and industry members. It is recommended that each asset owner identify an individual who can receive this information and further disseminate within the organization, so that actions can be taken to mitigate risks.

Question 19:

Q: Do you conduct regular security incident drills? This may be tabletop cyber exercises, active shooter drills, etc.

What are these drills?

Security incident drills are mock incidents that test the accuracy and knowledge of response procedures. These drills may be tabletop drills or interactive sessions. These may be cyber or physical security. These are required in some regulated environments and are recommended, typically annually, in most security standards and guidelines.

Question 20:

Q: Is security, like safety, a topic included in business decisions, project planning, and budgetary planning?

How might security be included in these activities?

Security is often approached like safety- an integral part of daily activities to ensure operations are stable. To ensure this is the case, security should be considered when making decisions around technology, vendors, acquisitions, and in procurement activities. Project planning should include risk assessment of design and changes to security controls, technology, and operations. Lastly, security, like safety, requires a budget that supports implementation and management of technical controls, training, drills, etc.

Question 21:

Q: Do you feel there is a "culture of security" and general awareness of security in your organization?

What is meant by a "culture of security"?

Security, like safety, should be ingrained across all aspects of the organization and daily operations. This could be considered a core organizational value, ensuring the safety and stability of operations. An awareness of security, shared across the organization, ensures that employees are vigilant and safe and operational processes remain secure.

Question 22:

Q: Does your organization regularly conduct cyber vulnerability assessments (or pen tests)?

What is a cyber vulnerability assessment or pen test?

Vulnerability assessments are typically investigations of the network, systems, and OT components that identify risks and weaknesses that may be exploited by an adversary. These may include configuration weaknesses, missing patches, weak policies, etc. Conducting these assessments commonly includes hands-on scans and investigation. Penetration tests, or 'pen tests', are hands-on activities where the assessment teams take the same actions as an adversary to determine the success of common threat vectors.

Question 23:

Q: Does your organization maintain a cyber asset inventory?

What is an asset inventory?

An asset inventory is a catalog of hardware and software components. This catalog denotes the asset location, make/model, version, and other data used to track, maintain, and protect important assets.

Question 24:

Q: Does your organization regularly conduct IT cyber security awareness training?

What is IT cyber security awareness training?

IT cyber security awareness training is designed to educate employees about cyber threats and good security practices that should be employed throughout daily activities. IT training focuses on business and enterprise systems. Many regulations, standards, and guidelines include training as required or recommended practice. In addition, insurers and auditors commonly ask about cyber security training and its occurrence at regular intervals. Training is often tracked as a compliance metric.

Question 25:

Q: Does your organization regularly conduct OT cyber security training for those with elevated system or network privileges?

What is OT cyber security awareness training for those with elevated privileges?

In addition to IT cyber security awareness training, OT cyber security training is a required or recommended practice. Due to OT's critical nature and advanced protection, those with administrative access, or those responsible for OT systems, should be aware of security threats and required mitigations. OT training is focused on those critical OT systems and designed for a reduced audience who have a need-to-know.

Question 26:

Q: Does your organization administer training on social engineering, social media usage, and phishing?

What is training on social engineering, social media usage, and phishing?

Adversaries use common threat vectors and tactics which are often successful to an unsuspecting user. Social engineering and phishing are two common activities. Collecting information about a user via social media is also common. When employees are trained on these threat vectors, they can spot suspicious activities and prevent the adversary's success.

Question 27:

Q: In the event you received a suspicious email or call, phishing attempt, or possible cyber risk, does your organization have, and follow, clear and concise steps to take for reporting and responding to the risk?

Why is it important to report and respond to these risks?

Adversaries commonly target more than one user at an organization. More sophisticated adversaries choose specific targets in an organization based on their roles and responsibilities. It is important to have an organizational process to collect these reports, take mitigation steps, and engage with employees being affected. Without a reporting process, it may not be recognized that multiple users are being targeted, and the organization may not make decisions to react to the threat and mitigate the risks.

Question 28:

Q: In the event you identify a physical security situation, such as a suspicious package, OT equipment theft, or tampering of gates and doors, does your organization have, and follow, clear and concise steps to take for reporting and responding to that situation?

Why is it important to report and respond to these risks?

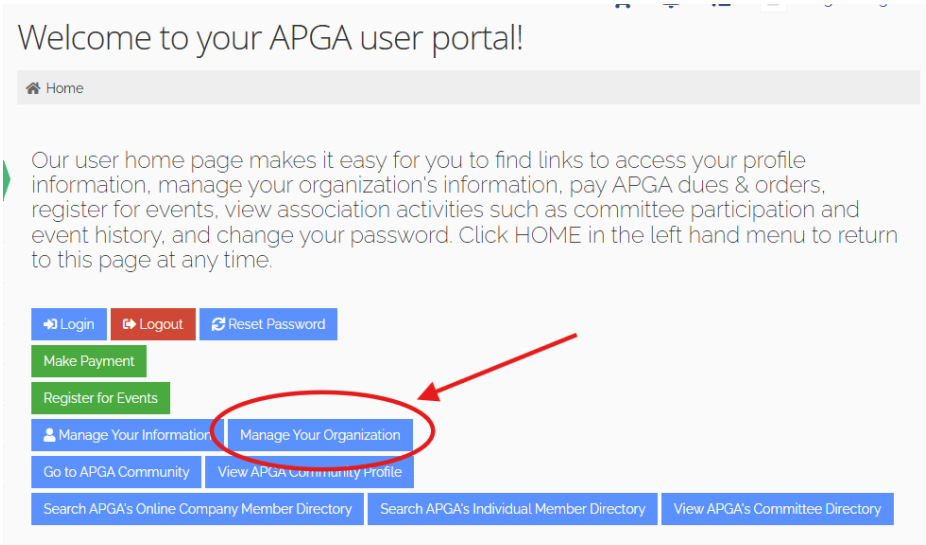
Physical security is essential to the safety and security of employees and sites, as well as the protection of digital assets. Like safety risks, all employees have the responsibility of reporting any security risks immediately to identified individuals. Investigating and responding to these reports should be a defined process within the organization.

Demographic Information

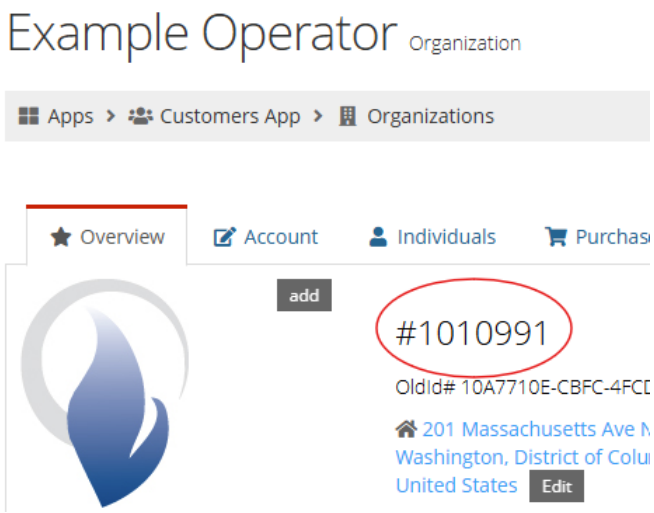
As mentioned in the front-matter of this document, the Security Self-Assessment Tool collects general demographic information about each submitter and their APGA Member ID such that APGA may identify submitters individually, should need arise.

How to locate my APGA Member ID

1. Login to the APGA User Portal: Welcome to your APGA user portal!
2. Select "Manage Your Organization" and then press the EDIT button next to your organization's name.



Your Company's Member ID will appear on the next page to the right of your image (or the image placeholder).



How do I find my PHMSA region?

Navigate to Offices | PHMSA to see a list of states by PHMSA region.

What is "Other" under Asset Types?

This option was provided in the case that the other two options did not adequately describe an operator. Use as you see fit.

Why is the commodity and utility type requested?

In the security environment, what commodities are involved have regulatory and practice implications. For instance, combined utilities have more exposure to both threats and regulations than gas-only utilities. Additionally, there may be security elements in place across other departments of the utility that can be leveraged for gas. For example, electric organizations that already have NERC-CIP programs are well positioned to share practices with gas departments.

The type of utility is a relevant data point because it helps to determine not only what regulatory oversight is applicable to a particular operator, but what financial models are in place. This helps with policy-informing information.

Scoring

This survey uses a simplified maturity model scoring. Generally, responses are assigned 1-4 points. Overall, the maximum score is the number of questions multiplied by 4. As published in Version 1 (Effective October 2025), the maximum possible score is 28 x 4 = 112.

Each respondent's score is tallied and presented out of the possible score. This score is intended to be indicative only. Low scores relative to the maximum likely indicate that an organization exhibits excess risk, and high scores likely indicate an organization that may be better prepared for security threats.

The goal of the scoring mechanism is to provide stakeholders with a score that allows each member to compare their readiness against an objective set of parameters and to allow benchmarking between respondents such that APGA may evaluate the relative readiness of members across broad demographic markers.

END