API Guidance Document

UTILIZING INTELLIGENCE TO SECURE PEOPLE, OPERATIONS and ASSETS

An Introduction to Uses and Sources

August 2015

API Guidance Document

UTILIZING INTELLIGENCE TO SECURE PEOPLE, OPERATIONS and ASSETS

An Introduction to Uses and Sources

Produced by the American Petroleum Institute
1220 L St NW, Washington, DC
www.api.org

August 2015

Utilizing Intelligence

Oil and natural gas industry operations span the globe in the exploration, production and distribution of vital energy resources. These resources can be located in areas with varying levels of infrastructure, government authority, and security for the general population, as well as industry workers and operations. These complicated environments require additional responsibilities and procedures by the industry to ensure their operations and personnel are safe and secure. Chief among these responsibilities is developing and maintaining situational awareness of the operating environment in areas where there may be limited information flow or operational control over external conditions. Gaining situational awareness, both domestically and in foreign countries, is a challenging task that takes coordinated action by companies with their personnel and potentially with the U.S. government and foreign or host governments.

Understanding how information and intelligence is collected, assessed, and applied is fundamental to developing and maintaining robust situational awareness. While intelligence collection and use is traditionally considered an inherently governmental function, companies that operate in environments where the safety of workers and operations are vulnerable to security related externalities have a responsibility to utilize the information and intelligence available to them to guide their actions. There are many sources of information available to private companies, including intelligence supplied by governments, from public-private information sharing groups, private intelligence firms, open (i.e. unclassified) sources, and sometimes from intelligence analysts working directly for the industry. Knowing what these various sources are and understanding how to utilize them is the first step to creating situational awareness and responsible risk assessment and management.

Recognizing the Threats

Today's world is full of threats to the safety of operations and personnel, both domestically and abroad. Terrorism, civil unrest, crime, drug trafficking, armed conflict, cyber/information theft and extremism are all examples of threats that companies must understand and be aware of when setting up and maintaining operations throughout the world. While civil defense and law enforcement are the responsibility of government, protection of personnel, operations, capital, and intellectual property are all the responsibility of companies that employ and own those assets. Understanding the operating environment, through the collection and assessment of information and intelligence, provides companies with the situational awareness necessary to make sound choices.

Therefore, it is important for companies to understand how to utilize intelligence, what limitations may exist with it, and how to factor intelligence into the broader enterprise risk assessments and decision making processes. That said, an important caveat that companies must keep in mind when attempting to understand their operating risks is that there is no such thing as perfect intelligence. Intelligence is simply one of many important factors in decision making. Companies must also factor in other considerations such as risk tolerance, historical experience, political environments, and on the ground reporting from employees and contractors, among others. In addition, intelligence is often collected with specific criteria for specific purposes and may not be delivered to external stakeholders with the context in which it was collected. Companies must develop and maintain a level of sophistication related to the collection and use of intelligence in order to use it effectively for the protection of personnel and resources.

The FBI defines intelligence in the following way:

"Simply defined, intelligence is information that has been analyzed and refined so that it is useful to policymakers in making decisions—specifically, decisions about potential threats to our national security.

The FBI and the other organizations that make up the U.S. Intelligence Community use the term "intelligence" in three different ways:

- Intelligence is a product that consists of information that has been refined to meet the needs of policymakers.
- Intelligence is also a process through which that information is identified, collected, and analyzed.
- And intelligence refers to both the individual organizations that shape raw data into a finished intelligence product for the benefit of decision makers and the larger community of these organizations."

Private sector organizations fall into the third definition, as part of the larger community served by intelligence organizations. It is critical that companies understand this as they begin to utilize intelligence in decision making, even when it is shared directly between an agency and an operator. The U.S. government has a duty to inform affected parties when they believe intelligence detects a threat to people or operations but that intelligence may not reveal the full situation.

Government's Duty to Inform

The U.S. government has unique and extensive resources to collect and assess intelligence about a wide array of potential threats to the national interest. The U.S. intelligence community consists of sixteen separate agencies with various remits and responsibilities. Many collect, analyze and disseminate intelligence and threat information that relate to or impact operations and people in the private sector. When such intelligence exists or threats are known, the government has a duty to inform those who are directly affected, be they people or companies. Domestically, the Federal Bureau of Investigation (FBI) has the lead to contact companies or individuals to share the pertinent information that may affect their operations or safety. Notification to U.S. companies and citizens operating overseas is more complicated but is typically managed through U.S. embassies. It is critical to understand, that while the government has a duty to inform, companies have a responsibility to make sure they have the appropriate personnel in place and the necessary relationships to receive information when it is available.

While the government has a duty to inform, companies have a responsibility to make sure they have the appropriate personnel in place and the necessary relationships to receive information when it is available.

Public Sources of Intelligence and Threat Information

The following will document the various ways by which companies can engage to receive, collect, and understand the information necessary to provide situational awareness and safe operating environments throughout the world.

Overseas Security Advisory Council (OSAC)

The Overseas Security Advisory Council is a partnership between the U.S. Department of State and private sector entities, "to promote security cooperation between American private sector interests worldwide and the U.S. Department of State." OSAC partnerships and activities exist both at the U.S. federal and country level. Private sector entities can participate in OSAC meetings, working groups, events and threat reporting domestically or through membership in regional councils in more than 140 countries. The Council's design provides flexibility to members, allowing each to customize the information they wish to receive through their membership and level of engagement. A primary benefit of participation in overseas councils is engagement with U.S. embassies. As companies engage with embassies in their countries of operations, the embassies can reach out directly to provide relevant and timely threat information specific to the country, operations, and personnel. This information can often be critical, particularly if country evacuations, enhanced security procedures or emergency response operations are required.

For more information, visit https://www.osac.gov/Pages/Home.aspx.

Domestic Security Alliance Council

The Domestic Security Alliance Council (DSAC) is an initiative of the Federal Bureau of Investigation (FBI), in partnership with the Department of Homeland Security (DHS) and the private sector to improve prevention, detection and deterrence of criminal acts. Created after 9/11 and modeled after OSAC, DSAC attempts to coordinate threat information and reporting with the larger intelligence community and the private sector domestically through outreach, regional engagements, training and education. Also similar to OSAC, membership in DSAC creates the channels between the government and the private sector that facilitate timely, relevant sharing of critical security and threat information. Government and private sector analysts meet regularly to discuss threats, enhancing the government's understanding of industry operations and what information is critical and relevant.

For more information, visit http://www.dsac.gov/Pages/Index.aspx#.

Law Enforcement Enterprise Portal (LEEP)

The FBI built the Law Enforcement Enterprise Portal (LEEP) to be the cyber gateway to a number of unclassified services for law enforcement, intelligence groups, and criminal justice entities. One of the services is Law Enforcement Online (LEO). Other services on the portal include: FBI Special Interest Groups (SIGs) and Virtual Command Centers (VCCs); the Internet Crime Complaint Center (IC3); the National Data Exchange (N-DEx); Joint Automated Booking System (JABS); Intelink (U), and RISSNet.

The noted services are primarily for local, state, tribal, and federal law enforcement; however, InfraGard and its partner iLEEP (including CyberHood Watch) and iGuardian are FBI affiliated web services that specialize in coordination with

private sector security interests for Cyber related threats. There are also several public/private enforcement activities managed in a LEO SIG on the LEEP portal. In these circumstances, private sector members can be given limited access to their particular project on the law enforcement site. For example, when multiple local law enforcement agencies, security firms, FBI field offices, and related private sector services begin experiencing an increase in crime a SIG can be created to allow all those parties to access and share information in a secure and timely manner. Though legal barriers exist on LEEP to protect civil rights and privacy interests, as well as the confidential nature of most law enforcement investigations, there are circumstances in which public officers and private sector personnel can work together effectively and legally on the FBI's unclassified portal, LEEP.

For more information please see the LEEP portal at www.cjis.gov.

Infragard

Similar to DSAC, Infragard is focused on domestic threats, but primarily as they relate to cyber security. "It is an association of persons who represent businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the U.S." Infragard is organized into chapters at the city and regional level, commensurate with the FBI field offices to provide direct, in person communication between Infragard members and FBI agents. Infragard shares information and alerts, holds meetings and forums to provide education to stakeholders, and engages in outreach to nonmembers to grow the information sharing community.

More information can be found at https://www.infragard.org/.

Homeport

Homeport is the U.S. Coast Guard's (USCG) portal to information and services. Limited to owners, operators, and members of USCG security or safety committees, Homeport provides threat information and security and safety information related to ports, vessels, waterways and coastal issues.

For more information, visit https://homeport.uscg.mil.

US-CERT

The United States Computer Emergency Readiness Team (US-CERT) leads efforts to improve the nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the Nation. Subscribing to US-CERT provides entities with technical assistance, timely notifications regarding current and potential security threats and vulnerabilities, and collaborative response to incidents.

For more information, visit https://www.us-cert.gov/.

ICS-CERT

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) partners with law enforcement agencies and the intelligence community and coordinates efforts among Federal, state, local, and tribal governments and control systems owners, operators, and vendors. Additionally, ICS-CERT collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures. Subscribing to ICS-CERT provides private sector entities with access to reporting, training, recommended practices, assessments and other standards and references to help entities protect their control systems.

For more information, visit https://ics-cert.us-cert.gov/.

Fusion Centers

State and major urban area fusion centers (fusion centers) serve as focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information between the federal government and state, local, tribal, territorial (SLTT) and private sector partners.

Located in states and major urban areas throughout the country, fusion centers empower front-line law enforcement, public safety, fire service, emergency response, public health, critical infrastructure protection, and private sector security personnel to understand local implications of national intelligence. They conduct analysis and facilitate information sharing while assisting law enforcement and homeland security partners in preventing, protecting against, and responding to crime and terrorism. Fusion centers are owned and operated by state and local entities with support from federal partners in the form of deployed personnel, training, technical assistance, exercise support, security clearances, connectivity to federal systems, technology, and grant funding.

For more information, visit http://www.dhs.gov/state-and-major-urban-area-fusion-centers or https://nfcausa.org.

Homeland Security Information Network

The Homeland Security Information Network (HSIN) is a portal created and supported by DHS to deliver Sensitive But Unclassified (SBU) to stakeholders throughout the Unites States. HSIN provides the participants alerts and notifications access to government documents, and a forum for information sharing at a level of security not open to the public. Many critical infrastructure sectors, including oil and natural gas, have created Communities of Interest (COIs) within the HSIN portal to share sector specific information. These portals can be useful to sectors as they develop materials relevant to others and to serve as a repository for historical information.

More information can be found at http://www.dhs.gov/homeland-security-information-network.

Foreign Country Intelligence

Organizations that operate internationally and those that have headquarters or offices in foreign countries should also consider tapping into foreign sources of intelligence. Governments around the world often have robust intelligence services that support the safety and stability of their societies and economies. As with U.S. embassies abroad, forming relationships and making connections with host country governments can facilitate the timely and effective sharing of relevant threat information. It should be noted that not all host country governments have robust intelligence services available to private interests and any engagement with a foreign host should be made carefully.

Private Sector Security Clearances and Classified Briefings

For those entities engaged in operations that require information sharing at a secure level, the Federal government has several programs that provide private sector personnel access to an official U.S. government security clearance. Often during an imminent, company specific event, government representatives can share critical classified information to mitigate a threat. However, companies can proactively engage with the intelligence community by requesting clearances for those personnel with the greatest need to know, typically physical security managers or those responsible for information technology or industrial control system security. Possession of a security clearance allows participation in classified briefings. Briefings are held typically held regionally or by sector. DHS, TSA, USCG, DOE and FBI all provide clearances to members of the oil and natural gas community.

Private Sources and Programs

Internal Capabilities

Private sector entities can develop internal analytical capabilities using open source or foreign based information to focus on the issues and areas that are most important to their operations. While building in-house capabilities does require a resource commitment, it is a means to gather and analyze the information most germane to an entity with operations in sensitive or risky areas, operations or industries that may be known targets, or those that require additional information for risk assessment and security planning.

Private Intelligence Firms

For those entities that require customized intelligence analysis and products but do not have the desire or resources to create internal capabilities, there are many private intelligence firms in the marketplace. Private intelligence firms can provide a significant range of products and may have certain specialties, such the Middle East, internet security, or terrorism. Private sector entities should assess their resources, capabilities, and needs to determine what provider best suits their needs.

For those entities engaged in operations that require information sharing at a secure level, the Federal government has several programs that provide private sector personnel access to an official U.S. government security clearance.

Information Sharing and Analysis Centers

The oil and natural gas sector has formed an Information Sharing and Analysis Center (ONG ISAC). ISACs are established to provide comprehensive sector analysis, which is shared within the sector, with other sectors, and with governments, dependent on the remit of each ISAC. Services provided by ISACs include risk mitigation, incident response, alert and information sharing. The ONG ISAC was created to provide shared intelligence on cyber incidents, threats, vulnerabilities, and associated responses present throughout the industry. Membership in the ONG ISAC includes secure information sharing, threat indicators, and access to analysts. Natural gas utilities participate in the Downstream Natural Gas ISAC (DNG ISAC), which focuses on cyber and physical security incident information and closely coordinates with the Electric Subsector ISAC.

For more information, visit http://ongisac.org/ and https://www.dngisac.com.

Intelligence Analysis and Actions

Vetting & Verifying

As stated earlier, there is no such thing as perfect intelligence. Therefore, it is critical that as organizations develop their risk analyses using intelligence products, they also consider the various environmental factors that affect security and operations. Security risk is a function of potential consequence, risk to assets and threats. To ensure planning is done effectively and efficiently, organizations need to vet and verify intelligence as it relates to their operating environments, risk profile and risk tolerance, and when possible, their personnel on the ground. Utilizing intelligence should be part of a larger security program by skilled professionals who understand their operating environments and how to respond to changing threats.

Organizations operating overseas should form a relationship with the local U.S. embassy.

Working with U.S. embassies

As a best practice, organizations with a US interest, operating overseas, should form a relationship with the local U.S. embassy. When relationships are established and embassies are aware of U.S. companies and personnel traveling or operating in their area of responsibility, the embassies can provide timely and often critical information. Conversely, if there are known threats and an individual have not communicated with the local embassy, there is no means to communicate threat information or country alerts with that individual. While the government has a duty to inform, individuals and organizations have a responsibility to engage to receive the information.

Handling Intelligence

Organizations need to ensure that they are aware of and following the handling practices appropriate or required for the types of intelligence they are receiving or collecting. The U.S. government, as do most governments, has strict requirements for the handling, dissemination, and storage of intelligence that all clearance holders must follow in order to protect the intelligence and to maintain their clearances. Typically, penalties for improper handling or dissemination of intelligence involve the loss of privileges, fines and in some cases, incarceration. For those organizations that are utilizing open source intelligence, intelligence from private sources, or other sensitive but unclassified intelligence, such as Law Enforcement Sensitive intelligence, they should develop internal protocols to handle and protect the intelligence products. Generally, sharing of intelligence is based on a need to know and protections of the intelligence are based on the harm done if the information were improperly shared. Organizations should consider the potential impact of disclosure when designing their protocols.

Traffic Light Protocol

The Traffic Light Protocol (TLP) is a set of designations used to ensure that sensitive information is shared with the correct audience. It employs four colors to indicate different degrees of sensitivity and the corresponding sharing considerations to be applied by the recipient(s). The originator of information to be handled according to TLP should label the information with the correct TLP color in order to indicate how widely that information may be disseminated. TLP does not apply to classified information.

When should it be used?	Color	How may it be shared?
Sources may use TLP: RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	RED 	Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.
Sources may use TLP: AMBER when information requires support to be effectively acted upon, but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	AMBER 	Recipients may only share TLP: AMBER information with members of their own organization who need to know, and only as widely as necessary to act on that information.
Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	GREEN 	Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.
Sources may use TLP: WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	WHITE 	TLP: WHITE information may be distributed without restriction, subject to copyright controls.

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Conclusion

Creating a comprehensive security risk identification and analysis capability is a critical part of ensuring security for operations, personnel and assets. In today's interconnected and dynamic world, building a comprehensive picture must take into account many factors, including threats made against the industry domestically and abroad, threat actors, economic, political and societal environments, and the risk tolerance of an organization, among others. Intelligence is one critical resource that can be used to build this picture, and while not always perfect or comprehensive, organizations should understand what is available and how it can be utilized. There are many threats that can affect operations and personnel in the oil and natural gas sector, but not all may require action on the part of the operator. Organizations should have the capability to make those decisions when they are faced with them. Key aspects of that capability are understanding what resources are available, having the relationships in place to receive and respond to intelligence, and building the capacity to effectively vet and verify when action is required.

i. http://www.fbi.gov/about-us/intelligence/defined
ii. https://www.osac.gov/pages/aboutus.aspx
iii. https://www.infragard.org/