ATA

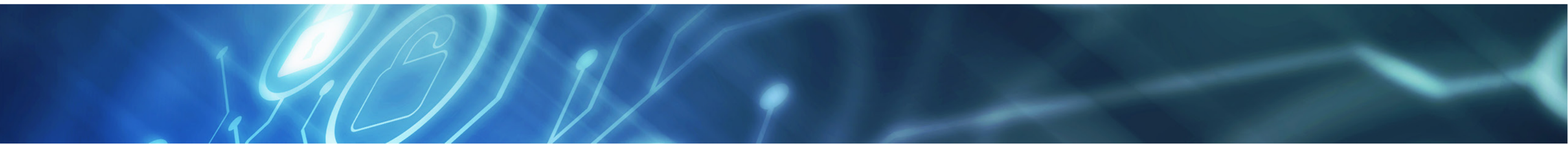
FLEET CYWATCH

TMC

Transportation Security Council

COUNCIL OF

ATA AMERICAN TRUCKING ASSOCIATIONS



Program Overview

Table of Contents

I. Executive Summary

Advanced computing and connectivity are critical components of commercial vehicle safety systems, powertrain controls, and operating communications. The trucking industry increasingly relies upon these technologies for improved operations, company growth, and to meet federally mandated regulations. While these technologies can improve emergency service, traffic congestion, and help support the growing demand for transportation of freight, concern exists about potential disruption from cyber-attacks. Therefore, as safety is the American Trucking Associations' (ATA) first priority for the trucking industry, initiating a motor carrier-based program – Fleet CyWatch – that identifies emerging cyber threats and helps guard against malicious actions of cyber criminals is of vital importance to ATA fleet membership.

Fleet CyWatch is an ATA Technology & Maintenance Council (TMC) and Transportation Security Council (TSC) supported program that assists fleet members in reporting information about trucking related internet crimes and cyber-attacks, and shares information to fleets about cyber threats that may impact their operations. Fleet CyWatch will coordinate with private and federal efforts to provide motor carriers with information and recommendations in the areas of cybersecurity awareness, prevention, and mitigation methods. The Program connects industry, federal enforcement, and associations and trade groups specialized in cybersecurity to improve U.S. road transport safety.

As a free member benefit to motor carriers belonging to ATA or its Councils, using Fleet CyWatch is recommended for reporting all types of internet crimes related to disrupting fleet operations. Reports will be communicated with appropriate federal cyber-authorities to be handled by jurisdiction, type of cybercrime, and commercial/public impact. After protecting fleet identity, reports are communicated with intelligence sharing and analysis agencies and the fleet community registered to Fleet CyWatch. Responding alerts through Fleet CyWatch will address cybersecurity training and education, cyber-threat trends and patterns, and best practices development. Relative and developing standards will be communicated also.

The Fleet CyWatch program also seeks to improve public awareness of industry and government efforts to prevent potential terrorist acts using commercial vehicles as instruments by way of cyber-attack. Effective implementation of the Program will create a dynamic, vibrant program with members who are engaged in the cybersecurity issues most important to the trucking industry.

II. Introduction

Advanced computing and connectivity are critical components of commercial vehicle safety systems, powertrain controls, and operating communications. The trucking industry increasingly relies upon these technologies for improved operations, company growth, and to meet federally mandated regulations. While these technologies can improve emergency service, traffic congestion, and help support the growing demand for transportation of freight, concern exists about potential disruption from cyber-attacks. Today's fleet executive expects to be connected, whether at home, work office, or in the truck for maintenance updates, delivery schedule, cargo awareness, and driver hours of service. As we move toward an increasingly interconnected future, motor carriers should prepare to address the complexities and challenges that come along with the benefits of connectivity and advanced technology.

Concurrent with the increasing connectivity in society and business, we are seeing an increase in cyber-crime. In May 2000, the Federal Bureau of Investigation (FBI) established the Internet Crime Complaint Center (IC3) as a center to receive complaints of Internet crime. In June 2007, the IC3 received its one millionth complaint, two millionth in November 2010, and three millionth in 2014. As of 2016, there have been 3,762,348 complaints reported to the IC3 since its inception. Over the last five years, the IC3 received an average more than 280,000 complaints per year and that's an estimated 15 percent of the nation's fraud victims that report their crimes to law enforcement. In 2016, the IC3 received nearly 300,000 complaints in monitoring trending scams with reported losses in excess of $1.3 billion.

In today's environment, cyber adversaries target victims based on poorly secured systems and inexperienced employees to illegally access confidential and proprietary information, disrupt business operations, and leverage compromised systems for malicious purposes. The safety and security of on-road commercial vehicles is a top priority for ATA. To help protect the trucking industry from cyber-attacks and their negative consequences, ATA has established the Fleet CyWatch program. Fleet CyWatch serves to reduce the number of internet crimes involving the trucking industry through cybersecurity awareness, prevention, and mitigation. The Program connects industry, federal enforcement, and associations and trade groups involved in cybersecurity to protect U.S. road transport safety from cyber-threats.

Specifically, Fleet CyWatch will:

A. Facilitate information sharing among members regarding cyber-threats, countermeasures and best practices
B. Direct internet crime complaints to appropriate authorities
C. Coordinate with ATA's TMC Cybersecurity Issues Task Force – Fleet CyWatch Steering Committee
D. Utilize ATA's TSC membership and fleet incident notification awareness
E. Provide cybersecurity training and education
F. Survey and benchmark trucking cybersecurity programs
G. Enhance the image of trucking advanced technology through stakeholder, government, and general public connections

II. Mission Statement

The Fleet CyWatch mission is to reduce the impact and frequency of internet crimes and cyber-attacks in the trucking industry through the identification and sharing of information related to cyber adversaries and threats, cybersecurity best practices, automation protocols security in cyber-physical systems, and recommend relevant and developing NIST, SAE, and ISO standards.

IV. Description

ATA's Fleet CyWatch is a national TMC- and TSC-supported cybersecurity program, focused on providing motor carriers with cybersecurity information and recommendations that will make a positive difference in a fleet's cybersecurity and the public's trust of America's trucking industry. Fleet CyWatch can make a significant contribution to highway safety for truck drivers and the motoring public while enhancing the industry's image. It is member led and connected with private and federal efforts in cybersecurity awareness, prevention, and mitigation toward internet crimes and cyber-attacks in the trucking industry.

ATA and Council fleet members operating in the United States can access Fleet CyWatch through ATA's web site at fleetcywatch.trucking.org. If a fleet finds itself under any circumstance in the action of cyber-criminal activity affecting their operations, they may log into ATA, enter the Fleet CyWatch web site, and submit a Cyber Incident Report. This Report will be communicated with appropriate federal law enforcement to be handled by jurisdiction, type of cybercrime, and fleet/public impact. The Report is also anonymized to protect fleet identification then communicated with information sharing agencies and additional cyber resources. Fleet CyWatch subscribers will be updated with cyber resource solutions as the Report is tracked by ATA Fleet CyWatch staff in anonymous condition. After enough Reports and analysis is completed within an acceptable timeline, a Study – ATA's Fleet CyWatch Study – will be developed and made available for Fleet CyWatch subscribers. The Fleet CyWatch Study will provide ATA & Council members with a review of cybercrime trends and new prevention methods in trucking cybersecurity.

Additionally, after a Report is submitted, a Cyber Incident Response Open Notification will be generated, verified, and anonymized for distribution to ATA fleet members to raise awareness. After either:

a) the originating fleet user is satisfied with ATA's Fleet CyWatch services;

b) the fleet is able to return to normal operating status;

c) the cybercrime was resolved, or;

d) the cyber-resources providing reporting services to Fleet CyWatch (see below) have exhausted all means and have developed their best conclusions.

Finally, a Cyber Incident Response Closed Notification will be generated and anonymized for distribution to Fleet CyWatch members.

The following federal law enforcement and intelligence sharing agencies are Fleet CyWatch optional reporting resources (depending on the details of a specific event):

- Fleetcywatch.trucking.org – ATA Fleet CyWatch program personnel.
- www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force – National Cyber Investigative Joint Task Force (NCIJTF) 24-hour cyber command center.
- www.fbi.gov/contact-us/field - The FBI has 56 field offices (also called divisions) centrally located in major metropolitan areas across the U.S. Depending on what state(s) the cyber-attack is reported in by the input of the Fleet CyWatch user, the assigned FBI cyber division will be notified.
- www.IC3.gov – The FBI's Internet Crime Complaint Center provides the public with a reliable and convenient reporting mechanism concerning suspected Internet-facilitated criminal activity and to develop effective alliances with law enforcement and industry partners. Information is analyzed and disseminated for investigative and intelligence purposes to law enforcement and for public awareness.
- www.infragard.org – InfraGard is a partnership between the FBI and members of the private sector (i.e., ATA). The InfraGard program provides a vehicle for seamless public-private collaboration with government that expedites the timely exchange of information and promotes mutual learning opportunities relevant to the protection of critical infrastructure.
- www.ncfta.net – The National Cyber-Forensics & Training Alliance (NCFTA) is a non-profit corporation, focused on identifying, mitigating, and neutralizing cyber-crime threats globally. The NCFTA operates by conducting real time information sharing and analysis with subject matter experts (SME) in the public, private, and academic sectors. Through these partnerships, the NCFTA proactively identifies cyber threats in order to help partners take preventive measures to mitigate those threats.
- www.surfacetransportationisac.org – The Surface Transportation Information Sharing & Analysis Center (ST-ISAC) collects, analyzes and distributes critical security and threat information from worldwide resources to protect its members' vital information and information technology systems from attack. The ST-ISAC is a secure reporting and analytical capability that, in addition to transmitting critical alerts, advisories and solutions, also provides a vehicle for the anonymous or attributable sharing of incident, threat, and vulnerability data.
- www.automotiveisac.com – The Automotive Information Sharing & Analysis Center (Auto-ISAC), originally for automakers to establish a secure platform for sharing, tracking and analyzing intelligence about cyber-threats and potential vulnerabilities around the connected light-duty vehicle, has extended membership to medium- and heavy-duty vehicle suppliers in early 2017.
- www.us-cert.gov/nccic– The National Cybersecurity and Communications Integration Center (NCCIC) is a 24/7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the Federal Government, intelligence community, and law enforcement.
- www.dhs.gov/homeland-security-information-network-hsin – The Homeland Security Information Network (HSIN) is the trusted network for homeland security mission operations to share Sensitive But Unclassified information. Federal, State, Local, Territorial, Tribal, International and Private Sector homeland security partners use HSIN to manage operations, analyze data, send alerts and notices, and in general, share the information they need to do their jobs.

A. Outline of Fleet CyWatch Reporting and Response Process

i. Fleets that are members of ATA and/or its Councils may join the Fleet CyWatch program and register a primary contact(s) to report cyber incidents.

   a. ATA Councils include: Technology & Maintenance Council (TMC), Safety Management Council (SMC), Transportation Security Council (TSC), National Accounting & Finance Council (NAFC), Information Technology & Logistics Council (ITLC)

ii. If a registered fleet recognizes an act of cyber-crime or suspects cyber-threat, they may report it through ATA's Fleet CyWatch website, fleetcywatch.trucking.org.

   a. A registered fleet authorized contact may complete and submit a Cyber Incident Report.

iii. After submitting the Report, Fleet CyWatch will communicate with the aforementioned reporting resources.

iv. After the Report is verified by the Program's reporting resources, initial response from certain agencies and ATA Fleet CyWatch staff will confirm Report delivery and next steps to the originating fleet.

v. After enough resources are used to prepare the Cyber Incident Response Open notification, one will be distributed to all Fleet CyWatch subscribers.

vi. Fleet CyWatch will then follow up with specific reporting resources for information sharing and intelligence briefing for TMC Recommended Practice development and updating the originating fleet as appropriate.

vii. After enough resources are used to prepare the Cyber Incident Response Closed Notification, one will be distributed to all Fleet CyWatch subscribers then the Report will close.

viii. Periodically, using anonymous and aggregated data, an ATA Fleet CyWatch Study may be published for electronic distribution to provide ATA and Council members with information on cybercrime trends and prevention methods.

V. Operations

A. Program Research

Extensive research has been conducted to obtain stakeholder input and to make sure the Program is launched on the right set of principles. Information obtained through ongoing assessments will be utilized to refine and clarify the structure, allowing the Program flexibility to meet the changing needs of fleet members. There will also be ongoing efforts to track the Program through time, providing statistics and general information for development of marketing communication efforts (e.g. public relations, advertising, collateral, newsletters, documentaries, etc.).

Ongoing research including surveys of carriers, shippers, truck manufacturers, technology suppliers, business providers, and public/private practitioners will be conducted periodically to gauge the acceptance, effectiveness, and direction of the Program.

B. Building National Relationships

For Fleet CyWatch to expand properly, the Program will focus on establishing credibility in building relationships with State Trucking Associations (STA). State members are important to the success of the Program as smaller carriers and technology/business providers may be more vulnerable to cyber-threats than larger entities. Exploitation of these vulnerabilities may have the potential to spread a cyber-attack across the larger industry. Fleet CyWatch will also actively engage with relevant government agencies and other stakeholders (e.g., standards organizations, regulating agencies, etc.) to share and receive information related to cybersecurity and cybercrime, and to collaborate in developing countermeasures, best practices, and industry standards as appropriate.

C. Membership and Recruitment

The Fleet CyWatch Program is designed exclusively for fleets as they are ultimately the end-user and highest at risk to potentially be a cyber-attack vessel to the public. Initially, the Program will only be available to fleet members and only to those contacts subscribed in the program – access by designated personnel.

A fleet member company to either ATA or its Councils may register and assign fleet personnel through the Fleet CyWatch website. ATA corporate fleet members may assign multiple designated personnel. Council individual fleet members may self-assign. ATA staff will monitor membership requests and manage registered users per fleet.

Fleet CyWatch member recruitment will be based on ATA motor carrier and Council fleet membership application forms. Member account benefit changes will also reflect Fleet CyWatch to be an option to join. Multiple member recruitment ads and image campaigns will run periodically through ATA and Council publications.

D. TMC and TSC Roles

ATA's Technology & Maintenance Council Cybersecurity Issues Task Force will host the Steering Committee for the Fleet CyWatch program to manage the general course of its operations – as outlined in Program Research. To ensure that the Program's mission and objectives are followed thoroughly, the Chairman of the Committee will work closely with the Program staff in developing TMC Recommended Practices and the prospective Fleet CyWatch Study.

ATA's TMC has developed a relationship with the FBI who is the lead United States Government agency for criminal cyber activity. The FBI Cyber Division Flash Notification alert system will be channeled through Fleet CyWatch to alarm subscribed users and to build on the Program's Cyber Incident Response Notifications.

ATA's Transportation Security Council supports government agencies to establish risk and education-based approaches when considering highway and motor carrier security measures. The TSC will support the Program's Cyber Incident Response notifications which allow members to quickly, privately and anonymously communicate incidents of internet crimes and cyber-attacks amongst themselves.

ATA's TSC also has developed a relationship with the Transportation Security Administration (TSA) who contributes to the Department of Homeland Security (DHS) cyber mission by assessing and updating cyber security protocols and programs to ensure the protection of both public and private data sources. The DHS US-CERT (Computer Emergency Readiness Team) notification alert system will be channeled through Fleet CyWatch to alarm registered users and to build on the Program's Cyber Incident Response notifications. Additionally, TSC will commit liaison members to the Steering Committee for consulting and advising carrier security operations.

E. Reporting Structure

For fleets to report cyber-crimes, users are urged to go on to ATA's website, www.trucking.org, TSC's website, http://tsc.trucking.org, or TMC's website, http://tmc.trucking.org, click on the Fleet CyWatch link, and fill in the appropriate levels of information describing their company's profile and the incident that has occurred in the Program's Cyber Incident Report.

The submitted Report will be analyzed and channeled through Fleet CyWatch reporting resources alerting correct federal authorities and intelligence agencies to what the incident consists of. ATA's Fleet CyWatch staff will be alerted of the Report and may contact the user as well as follow up with appropriate reporting resources. A Cyber Incident Response Open Notification will be created and logged until the incident has been concluded to give the user assurance and for developing counter measures.

Allowing Fleet CyWatch to assist in the user's Internet crime or cyber-attack lets TMC and TSC communicate in real-time over incidents submitted through this system which develops aggregated and anonymous Cyber Incident Response Notifications to the Fleet CyWatch membership. These Response notifications will inform Fleet CyWatch members of the incident and better prepare them with information on intrusion capabilities and preventive best practices. The Report allows Fleet CyWatch to establish trends involving:

- *what was hacked;*
- *how it was hacked;*
- *when it was hacked;*
- *where it was hacked;*
- *where the hacking came from;*
- *what departments did it affect;*
- *how/were customers affected;*
- *what counter measures were developed;*
- *what prevention methods worked/didn't work;*
- *how long was the hack in place on the user's system before it took effect;*
- *how long did it take to resolve;*
- *how was it resolved, and;*
- *what new measures are in place to prevent future occurrences.*

This allows ATA and Council members to share information, spot trends and work to stay ahead of the criminals.

VI. Outreach

General electronic-broadcast media and trade media stories and announcements will help support the Program and stimulate participation, sponsorship, and endorsements on an on-going basis. Stories may include: results of studies; Report histories about user resolutions over cybercrime; profiles on TMC Steering Committee participants; notable sponsorships; broadcasting Response notifications as they develop, and Q&A sessions with industry leaders in the Program.

VII. Key Program Elements

1. Private/Public Partner Participation -- Fleet CyWatch will seek to provide opportunities for active membership participation – to provide communication and security demonstrations to Fleet CyWatch participants.
2. Cyber Incident Response –A notification that Fleet CyWatch members receive by email through ATA's proprietary member account directory. The notification will inform subscribed Fleet CyWatch users that a cyber-incident occurred to an industry user. All details of the user will be anonymous except membership status, vocation, and industry specifics to better compare one's company. The incident details will be described and aggregated to secure the user's functions and educate members on pattern recognition. Notifications can be canceled through an unsubscribe option if the member desires.
3. Fleet CyWatch Study – ATA's Fleet CyWatch staff will periodically compile a study highlighting activities and progress of the Program. TMC's Steering Committee will approve the Study's direction and progress for pattern and benchmarking analysis.
4. Media Outreach – ATA staff will create and distribute a public service announcement to develop public awareness of the Fleet CyWatch program. Media will also be sought from traditional outlets through program launches and public interest stories.
5. Media Tracking – Public perception and knowledge of the Fleet CyWatch program will be created through earned media. Monitoring and collecting stories regarding the Program will assist managing it by identifying media messages and gauging public interest.

A. Potential Additional Program Elements

1. Cybersecurity Scholarship – ATA may seek to organize an educational scholarship for a Fleet CyWatch participant company – one of their employees to receive a cybersecurity supply chain advanced degree. This scholarship will be pursued for sponsorship availability.
2. Free Bug Bounty Services –To create a dynamic national membership team of professional white hat pro-trucking hackers that will instigate free bug bounty services for the industry.

VIII. For More Information

For additional information, please contact:

Ross Froat
Director, Engineering & IT
American Trucking Associations
950 N. Glebe Road
Arlington, Virginia 22203
(703) 838 – 7980

IX. Fleet CyWatch Report Example

FLEET CYWATCH INCIDENT NOTIFICATION

Date: (date of report given)

CIN#: (Cyber Incident Notification number given)

Motor Carrier member information: (provided with login)

Reporting individual information:
Name:
Job Title:
Phone:
Email:
Company (if not the same above):

Date of cyber-incident:
Location(s) of cyber-incident (user may enter more locations after logging an initial):
Business Name, Street Address, and City:
State and Zip Code:

Details of cyber-incident:
Equipment related (describe: makes, models, etc.):
Back-office related (describe: types of network, software, security, etc.):
Data corruption related (describe):
Is there indication of ransomware (describe):
Is this a result of spear phishing (describe):
Were there mitigation steps taken (if any):
Was there monetary loss or risk of (if any):

How were you or your company notified of the cyber-incident?

Is there indication of how or where the intrusion came from?

What departments of your fleet did it affect?

Prior to the FBI responding to a cyber incident, the items in the checklist below would greatly enhance the FBI's ability to investigate:

- Network inventory
- Software inventory
- Patch level of software
- Current Network Topology
- Network logs (i.e. DNS/VPN/Firewall)
- Host-based logs (i.e. web/firewall/AV)
- Secure email logs
- Domain Infrastructure/Group Policy
- Access Control Details
- List of external and internal IP addresses
- Physical/badge access logs
- Legal Banner Agreement

Please provide any additional information regarding the list above:

It is recommended by DHS that you keep any evidence you may have related to your complaint. Evidence may include, but is not limited to, the following:

- Canceled checks
- Credit card receipts
- Money order receipts
- Certified or other mail receipts
- Wire receipts
- Virtual currency receipts
- Pre-paid card receipts
- Envelopes (if you received items via FedEx, UPS, or U.S. Mail)
- Facsimiles
- Pamphlets or brochures
- Phone bills
- Printed or preferably electronic copies of emails (if printed, include full email header information)
- Printed or preferably electronic copies of web pages
- Hard drive images
- PCAP files containing malicious network traffic
- Network, host system, and/or security appliance logs
- Copies of malware
- Chat transcripts and/or telephony logs

Keep items in a safe location in the event you are requested to provide them for investigative or prosecutorial needs.

Any other relevant information you believe is necessary to support your complaint
(attachments available here):

Note: After submitting this report, notifications may be sent to:

- ATA Fleet CyWatch
- National Cyber Investigative Joint Task Force (NCIJTF) Cyber Watch Command Center
- FBI Local Office & Cyber Division of incident reported location(s)
- FBI Internet Crime Complaint Center (IC3)
- InfraGard
- The National Cyber-Forensics & Training Alliance (NCFTA)
- The Surface Transportation Information Sharing & Analysis Center (ST-ISAC)
- Automotive Information Sharing & Analysis Center (Auto-ISAC)
- National Cybersecurity and Communications Integration Center (NCCIC)
- Homeland Security Information Network (HSIN)

After you file a report with ATA's Fleet CyWatch, the information is reviewed by private and federal analysts and forwarded to federal, state, or local law enforcement with jurisdiction. ATA staff does not conduct investigations and, therefore, is not able to provide the investigative status of a submitted Report. Investigation and prosecution is at the discretion of the receiving cyber resources. Fleet CyWatch will monitor and follow up with the user depending on the level of cyber-incident and in accordance of the receiving cyber resources.

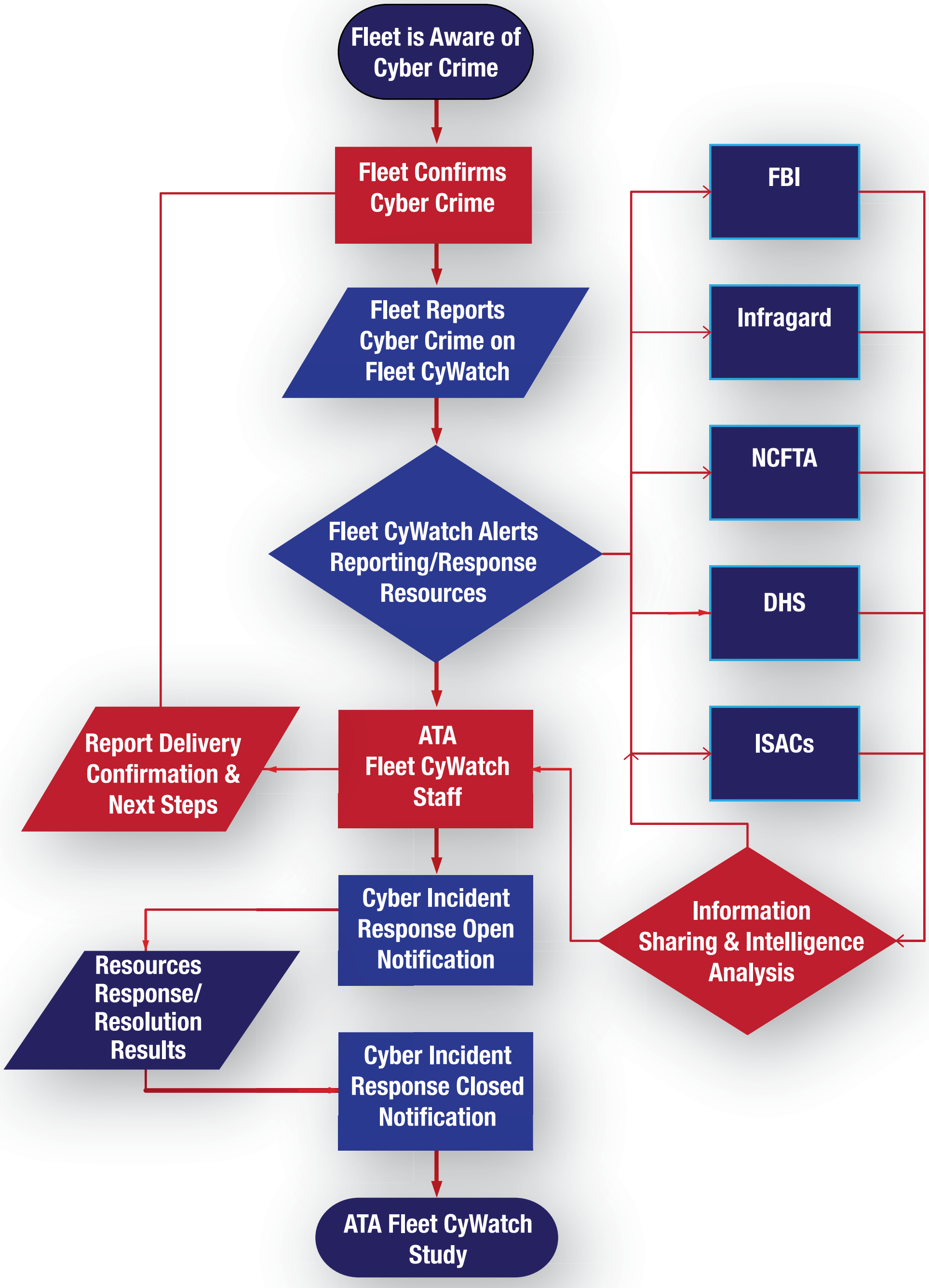
If you require immediate assistance, please contact your local FBI office from the provided list at https://www.fbi.gov/contact-us/field-offices, and local U.S. Secret Service Field Office and Electronic Crimes Task Force at http://www.secretservice.gov/contact/field-offices.
Also contact the NCCIC asset response line (888-282-0870).

User Agreement: You certify that the above information is to the best of your knowledge and that you are qualified within your company to provide such information.

Please contact Fleet CyWatch with any questions related to this Cyber Incident Notification at (703) 838-1700.

[Submit]

X. Fleet CyWatch Flowchart Example


Fleet is Aware of Cyber Crime
Fleet Confirms Cyber Crime
Fleet Reports Cyber Crime on Fleet CyWatch
Fleet CyWatch Alerts Reporting/Response Resources
FBI
Infragard
NCFTA
DHS
ISACs
ATA Fleet CyWatch Staff
Report Delivery Confirmation & Next Steps
Information Sharing & Intelligence Analysis
Cyber Incident Response Open Notification
Resources Response/ Resolution Results
Cyber Incident Response Closed Notification
ATA Fleet CyWatch Study