RadarFirst

CYBERSECURITY NOTIFICATION OBLIGATIONS

Transportation | U.S. Federal

Disclaimer

The information provided in this presentation does not, and is not intended to, constitute legal advice; instead, all information, content, and materials available in this presentation are for general informational purposes only. Information in this presentation may not constitute the most up-to-date legal or other information. This presentation contains links to third-party websites. Such links are only for the convenience of the reader; RadarFirst does not recommend or endorse the contents of the third-party sites.

INTRODUCTION

When cyber incidents occur, organizations have a responsibility to report them to various agencies, partners, and stakeholders.

In a recent report, the Department of Homeland Security found that there are **52 cyber incident reporting requirements, either in effect or proposed, across the Federal Government and 22 agencies**.

Current requirements are derived from a patchwork of regulations and authorities, many with **unique and sometimes overlapping information requirements**, timelines, and submission methods.

To simplify U.S. Federal reporting for Transportation organizations, RadarFirst has collected the following **16 effective and proposed reporting requirements** for cybersecurity notification obligations, their timelines, triggers, and reporting thresholds.

RadarFirst offers automation of risk assessment, third-party contract management, and notification guidance.

RadarFirst

REGULATIONS

CISA

- Chemical Facility Anti-Terrorism Standards (CFATS) (In Effect) *
- Rulemaking pursuant to the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (Under Development) **

USCG

- Suspicious Activity, Breaches of Security, or Transportation Security Incidents (33 C F R 101.305 and CG-5P Policy Letter 08-16) *
- Hazardous Conditions (33 C F R 160.216) *
- Evidence of Sabotage or Subversive Activity (33 C F R 6.16-1) *

TSA

- Enhancing Public Transportation and Passenger Railroad Cybersecurity (In Effect) *
- Enhancing Surface Transportation Security (In Effect) *, Surface Transportation Information Circular 2021-01 *
- Enhancing Pipeline Cybersecurity Security Directive (SD) Pipeline 2021-01 series *
- Enhancing Pipeline Cybersecurity (In Effect) Information Circular Pipeline 2022-01 *
- Enhancing Rail Cybersecurity" (In Effect) Security Directive 1580-21-01 series *
- Airport Security Program (ASP) (In Effect) *
- Aircraft Operator Standard Security Program (AOSSP) *, Aircraft Operator Standard Security Program (AOSSP) *, Twelve Five Standard Security Program (TFSSP *), Private Charter Standard Security Program (PCSSP) (In Effect) *
- Indirect Air Carrier Standard Security Program (IACSSP), Certified Cargo Screening Standard Security Program (CCSSSP) (In Effect) *

DoD

- Safeguarding Covered Defense Information and Cyber Incident Reporting (In Effect) DFARS 252.204-7012, Cyber incident reporting for cloud computing services (In Effect) (DFARS § 252.239-7010(d)) *
- (10 U.S.C. § 391 - U.S. Code - Unannotated Title 10. Armed Forces § 391) *
- (10 U.S.C. § 393 - U.S. Code - Unannotated Title 10. Armed Forces § 393) *

Obligation includes urgent notification, i.e. "promptly" or "as soon as possible."

* ***Obligations includes time-based notification.***

** / **/ ** ***Regulation includes multiple obligations, unique timelines, and/or unique recipients.***

RadarFirst

Cybersecurity and Infrastructure Security Agency (CISA)

Requirement	Entities Subject to Reporting Requirements → Timeline and Triggers	Reportable Cyber Incidents / Threshold
Chemical Facility Anti-Terrorism Standards (CFATS) (In Effect)	Chemical facilities possessing high-risk substances → Must report incidents **promptly** after a cyber incident is identified	Any incident: • With malicious intent to adversely affect operations of critical cyber assets, or that • Covers IT equipment used to provide security for the facility or to manage processes involving chemicals of interest (COI) or critical assets of the facility

RadarFirst

Cybersecurity and Infrastructure Security Agency (CISA)

Requirement

Rulemaking pursuant to the Cyber Incident Reporting for Critical Infrastructure Act of 2022
(Under Development)
6 USC § 681 et seq.

US-CERT Federal Incident Notification Guidelines

CISA Training

Entities Subject to Reporting Requirements → Timeline and Triggers

Covered Critical Infrastructure Entities:

→ Must report ransomware payment **to CISA and the FBI, no later than 24 hours** after the ransom payment is made.

→ Must report cyber intrusion impacts **to CISA and the FBI no later than 72 hours** after the cyber incident occurred..

Reportable Cyber Incidents / Threshold

Report incidents that:

- ***Actually*** or ***imminently*** **jeopardizes**, **without lawful authority**, the **integrity, confidentiality, or availability of information** or an information system
- Constitutes **a violation or imminent threat of violation of law**, **security policies,** security procedures, or acceptable use policies
- **Require response** according to the **Incident Response and Awareness Training**

RadarFirst

United States Coast Guard (USCG)

Requirement

Suspicious Activity, Breaches of Security, or Transportation Security Incidents (In Effect)
33 C F R 101.305 and CG-5P Policy Letter 08-16)

Entities Subject to Reporting Requirements → Timeline and Triggers

"Owners or operators of vessels, maritime facilities, and/or outer continental shelf facilities"

→ Must notify the USCG **immediately** upon occurrence of the activity and/or incident.

Reportable Cyber Incidents / Threshold

Includes:

- Breaches of security
- Suspicious activity
- Activities that may result in a transportation security incident.

See the CG-5P Policy Letter 08-16 to industry for examples requiring cybersecurity notification.

RadarFirst

United States Coast Guard (USCG)

Requirement	Entities Subject to Reporting Requirements → Timeline and Triggers	Reportable Cyber Incidents / Threshold
Hazardous Conditions (In Effect) (33 C F R 160.216)	"Owners agents, masters, operators or the person in charge of a vessel " → Must notify the USCG **immediately upon discovery of hazardous condition** with the requirement to remediate or mitigate the hazardous condition to the satisfaction of the Captain of the Port.	**Hazardous conditions** are noticed.

United State Coast Guard (USCG)

Requirement	Entities Subject to Reporting Requirements → Timeline and Triggers	Reportable Cyber Incidents / Threshold
Evidence of Sabotage or Subversive Activity (In Effect) (33 C F R 6.16-1)	"Vessel and facility owners or operators" → Must notify the USCG **immediately upon discovery of the evidence of sabotage or subversive activity**. The Captain of the Port may issue orders and require action related to the report.	Notify when witnessing evidence of **sabotage or subversive activity** endangering any vessel, harbor, port, or waterfront facility.

Transportation Security Administration (TSA)

Requirement

Enhancing Public Transportation and Passenger Railroad Cybersecurity (In Effect)

Security Directive 1582-21-01 series

Entities Subject to Reporting Requirements → Timeline and Triggers

"Owners or operators of passenger railroad carriers or rail transit system"

→ Must report incidents as soon as practicable, but no later than **24 hours** after the incident

Reportable Cyber Incidents / Threshold

Cybersecurity incidents that need to be reported include:

a. **Unauthorized access** of an Information or Operational Technology system
b. **Discovery of malicious software** on an Information or Operational Technology system;
c. **Activity resulting in a denial of service** to any Information or Operational Technology system
d. Any other **cybersecurity incident that results in operational disruption** to the Owner/Operator's Information or Operational Technology systems or other aspects of the Owner/Operator's rail systems or facilities
e. An **incident that has the potential to cause impact to a large number** of passengers, critical infrastructure or core government functions, or impacts to national security, economic security or public health and safety

RadarFirst

Transportation Security Administration (TSA)

Requirement

Enhancing Surface Transportation Security
(In Effect)

Surface Transportation Information Circular 2021-01

Entities Subject to Reporting Requirements → Timeline and Triggers

Each entity as follows:

- Passenger railroad carrier
- Public transportation agency
- Operator of a rail transit system that is not operating on track that is part of the general railroad system of transportation, including heavy rail transit, light rail transit, automated guideway, cable car, inclined plane, funicular, and monorail systems
- Tourist, scenic, historic, and excursion rail owner/operator, whether operating on or off the general railroad system of transportation.

→ Must report incidents **as soon as practicable**, but **no later than 24 hours after** an incident is identified

Reportable Cyber Incidents / Threshold

Cybersecurity incidents that need to be reported include:

a. **Unauthorized access** of an Information or Operational Technology system;
b. **Discovery of malicious software** on an Information or Operational Technology system;
c. **Activity resulting in a denial of service to any Information** or Operational Technology system;
d. **Any other cybersecurity incident that results in operational disruption** to the Owner/Operator's Information or Operational Technology systems or other aspects of the Owner/Operator's rail systems or facilities;
e. An incident that has the **potential to cause impact to a large number of customers, critical infrastructure or core government functions,** or impacts national security, economic security or public health and safety.

RadarFirst

Transportation Security Administration (TSA)

Requirement

Enhancing Pipeline Cybersecurity Security Directive (SD) Pipeline 2021-01 series

Entities Subject to Reporting Requirements → Timeline and Triggers

"**Owners or operators of a hazardous and natural gas pipeline or a liquefied natural gas facility** notified by TSA that their pipeline system or facility is critical."

→ **Must report** incidents **as soon as practicable**, but **no later than 24 hours** after an incident is identified

Reportable Cyber Incidents / Threshold

Cybersecurity incidents that need to be reported include:

a. **Unauthorized access** of an Information or Operational Technology system;
b. **Discovery of malicious software** on an Information or Operational Technology system;
c. **Activity resulting in a denial of service** to any Information or Operational Technology system;
d. **A physical attack** against the Owner/Operator's network infrastructure, such as deliberate damage to communication lines;
e. Any other cybersecurity incident that **results in operational disruption** to the Owner/Operator's Information or Operational Technology systems or other aspects of the Owner/Operator's pipeline systems or facilities;
f. Any other cybersecurity incident that has the **potential to cause operational disruption** that adversely affects the safe and efficient transportation of liquids and gases including, but not limited to impacts to a large number of customers, critical infrastructure or core government functions, or impacts national security, economic security or public health and safety.

RadarFirst

Transportation Security Administration (TSA)

Requirement

Enhancing Pipeline Cybersecurity
(In Effect) Information Circular Pipeline 2022-01

Security Directive of the Pipeline 2021-01 Series

Security Directive of the Pipeline 2021-02 Series

Entities Subject to Reporting Requirements → Timeline and Triggers

"**Owners or operators of a hazardous liquid and natural** gas pipelines not subject to the Security Directive of the Pipeline 2021-01 and Pipeline 2021-02 Series

→ **Must report** incidents **as soon as practicable**, but **no later than 24 hours after** the **incident** is identified.

Reportable Cyber Incidents / Threshold

Cybersecurity incidents that need to be reported include:

a. **Unauthorized access** of an Information or Operational Technology system
b. **Discovery of malicious software** on an Information or Operational Technology system
c. **Activity resulting in a denial of service** to any Information or Operational Technology system
d. Any other cybersecurity incident that results in o**perational disruption to the Owner/Operator's Information** or Operational Technology systems or other aspects of the Owner/Operator's pipeline systems or facilities
e. An i**ncident that has the potential to cause impact to critical infrastructure or core government functions, or impacts national security,** economic security, or public health and safety.

RadarFirst

Transportation Security Administration (TSA)

Requirement

"Enhancing Rail Cybersecurity" (In Effect) Security Directive 1580-21-01 series

Entities Subject to Reporting Requirements → Timeline and Triggers

Surface Transportation Freight Rail. Specifically: "Each freight railroad carrier identified in 49 C.F.R. 1580.101 and other TSA-designated railroads.

→ Must notify TSA **as soon as practicable, but no later than 24 hours** after a cybersecurity incident is identified

Reportable Cyber Incidents / Threshold

Cybersecurity incidents that need to be reported include:

a. **Unauthorized access** of an Information or Operational Technology system
b. **Discovery of malicious software** on an Information or Operational Technology system
c. **Activity resulting in a denial of service** to any Information or Operational Technology system
d. Any other cybersecurity incident that results in o**perational disruption to the Owner/Operator's Information** or Operational Technology systems or other aspects of the Owner/Operator's rail systems or facilities
e. An incident that has the potential to cause impact to a large number of customers or passengers (as applicable), critical infrastructure or core government functions, or impacts to national security, economic security or public health and safety.

Transportation Security Administration (TSA)

Requirement	Entities Subject to Reporting Requirements → Timeline and Triggers	Reportable Cyber Incidents / Threshold
Airport Security Program (ASP) (In Effect)	Airport operators → **Must report** incidents **as soon as practicable**, but **no later than 24 hours after** an incident is identified.	Incidents to report include an event that, without lawful authority, jeopardizes, disrupts or otherwise impacts, or is reasonably likely to jeopardize, disrupt or otherwise impact, the integrity, confidentiality, or availability of: • Computers; • Information or communications systems or networks; • Physical or virtual infrastructure controlled by computers or information systems; • An information resident on the system. "This definition includes an event that is under investigation or evaluation by the aircraft operator as a possible cybersecurity incident without final determination of the event's root cause or nature (such as malicious, suspicious, benign)."

RadarFirst

Transportation Security Administration (TSA)

Requirement

Aircraft Operator Standard Security Program (AOSSP)
Full All Cargo Aircraft Operator Standard Security Program (FACAOSSP)
Twelve Five Standard Security Program (TFSSP)
Private Charter Standard Security Program (PCSSP)

(In Effect)

Entities Subject to Reporting Requirements → Timeline and Triggers

Aircraft operators of passenger or cargo transports

→ Must report incidents **as soon as practicable,** but **no later than 24 hours after** the incident is identified.

Reportable Cyber Incidents / Threshold

Incidents to report include an event that, without lawful authority, jeopardizes, disrupts or otherwise impacts, or is reasonably likely to jeopardize, disrupt or otherwise impact, the integrity, confidentiality, or availability of:

- Computers;
- Information or communications systems or networks;
- Physical or virtual infrastructure controlled by computers or information systems;
- An information resident on the system.

"This definition **includes an event that is under investigation or evaluation by the the CCSF** as a possible cybersecurity incident without final determination of the event's root cause or nature (such as malicious, suspicious, benign)."

Transportation Security Administration (TSA)

Requirement

Indirect Air Carrier Standard Security Program (IACSSP),

Certified Cargo Screening Standard Security Program (CCSSSP)

(In Effect)

Entities Subject to Reporting Requirements → Timeline and Triggers

Indirect Air Carriers (IACs), Certified Cargo Screening Facilities (CCSF)

→ Must report incidents **as soon as practicable**, but **no later than 24 hours after** the incident is identified.

Reportable Cyber Incidents / Threshold

Incidents to report include an event that, without lawful authority, jeopardizes, disrupts or otherwise impacts, or is reasonably likely to jeopardize, disrupt or otherwise impact, the integrity, confidentiality, or availability of:

- Computers;
- Information or communications systems or networks;
- Physical or virtual infrastructure controlled by computers or information systems;
- An information resident on the system.

"This definition **includes an event that is under investigation or evaluation by the CCSF** as a possible cybersecurity incident without final determination of the event's root cause or nature (such as malicious, suspicious, benign)."

RadarFirst

Department of Defense (DoD)

Requirement

Safeguarding Covered Defense Information and Cyber Incident Reporting
(In Effect)
DFARS 252.204-7012,

Cyber incident reporting for cloud computing services
(In Effect)
(DFARS § 252.239-7010(d))

Entities Subject to Reporting Requirements → Timeline and Triggers

Each **defense contractor** who:

- **Operates an unclassified information systems** that processes, stores, or transmits controlled unclassified information
- Is designated as **providing operationally critical support**

→ Must report cyber incidents **within 72 hours of discovery**

Reportable Cyber Incidents / Threshold

A cyber incident describes actions taken through the use of computer networks that:

- **Results in** a compromise or an actual or potentially **adverse effect on an information system and/or** the **information** residing **therein;**
- **Affects the contractor's ability to perform** the requirements of the contract that are designated as operationally **critical support.**

RadarFirst

Department of Defense (DoD)

Requirement

10 U.S.C. § 391 - U.S. Code - Unannotated Title 10. Armed Forces § 391 (In Effect)

Entities Subject to Reporting Requirements → Timeline and Triggers

Each **contractor, essential to** the **mobilization, deployment, or sustainment of** the **Armed Forces** in a contingency operation**. designated** by the Secretary of Defense **as a critical source of supply** for:

- **Airlift**
- **Sealift**
- **Intermodal transportation services**
- **Logistical support**

→ **Must report** cyber incidents **rapidly after a cyber incident occurs.**

Reportable Cyber Incidents / Threshold

A **cyber incident** describes **actions** taken **through** the use of **computer networks** that **result** in an **actual or potentially adverse effect on** an **information system or** the **information** residing **therein**.

Department of Defense (DoD)

Requirement	Entities Subject to Reporting Requirements → Timeline and Triggers	Reportable Cyber Incidents / Threshold
10 U.S.C. § 393 - U.S. Code - Unannotated Title 10. Armed Forces § 393 (In Effect)	**Any private entity granted** by the **Department of Defense** to **access, receive, or store classified information** for the purpose of bidding for a contract or conducting activities in support of any program of the Department of Defense → **Must report** cyber incidents **rapidly** after **network or information system** penetration.	The threshold consists of s**uccessful penetration of a network or information system** that contains or processes information created by or for the Department of Defense which requires enhanced protections from the contractor.

RadarFirst

Enterprise Value is at Risk

Existing tools and manual processes cannot scale with today's complexity.

Challenges

- Increased incident volumes
- Changing laws and regulations
- Assessment / decision consistency
- Short notification timelines
- Stretched resource capacity

Impact

- Missed notification deadlines
- Regulatory audits and fines
- Customer loss
- Significant external legal costs
- Staff retention / attrition

Outcomes

- Decreased enterprise value
- Brand / reputational damage
- Lost customer / partner loyalty
- Inability to scale
- High departmental overhead

Operationalize Notification Obligations with Radar® Compliance

Radar® Compliance is a rules and assessment engine that can be configured to satisfy internal and external compliance notification requirements and obligations, such as:

- Cybersecurity events
- Third-party contractual mgmt
- Auditable reporting
- And more

Talk to a RadarFirst specialist to learn how you can define your own notification triggers and obligations with **Radar® Compliance**.

Capital One · VOYA FINANCIAL · BNY MELLON · CNO FINANCIAL GROUP · Texas Capital Bank · RAYMOND JAMES · Hyundai Capital

Thank You!