Diligent

carahsoft.

Cyber Incident Regulations and Data Protection: What Governmental Organizations Need to Know

Thank you for downloading this Diligent solutions brief. Carahsoft is the Master GSA holder for Diligent cybersecurity solutions available via ITES-SW2, NASA SEWP V, NASPO and other contract vehicles.

To learn how to take the next step toward acquiring Diligent's solutions, please check out the following resources and information:

For additional resources:
carah.io/DiligentResources

For upcoming events:
carah.io/DiligentEvents

For additional Contrast solutions:
carah.io/DiligentSolutions

For additional Cybersecurity solutions:
carah.io/Cybersecurity

To set up a meeting:
Diligent@carahsoft.com
844-445-5688

To purchase, check out the contract vehicles available for procurement:
carah.io/DiligentContracts

For more information, contact Carahsoft or our reseller partners:
Diligent@carahsoft.com | 844-445-5688

Diligent carahsoft

Cyber Incident Regulations and Data Protection:

What Governmental Organizations Need to Know

As a government agency and mission-driven organization, valuable data moves through your networks each day, including budgets, financials and the personal details of taxpayers, service recipients, residents, constituents, employees, volunteers and other members of the public.

Cyber criminals are all too aware — and all too ready to make your good cause their next target. When they succeed, there's a lot at stake: your reputation, trust in public institutions, funding requirements and regulatory compliance with a growing array of legal requirements and policies.

As regulators respond to today's newest technologies and fast-evolving cyber threats — and place increasing focus on cyber resilience — organizations are being tasked to improve their ability to withstand, then quickly recover from cybersecurity incidents and to raise cybersecurity standards in key industries and their supply chains.

Some agencies may have resources available and could be making positive gains in cyber resilience, but others may be increasingly overwhelmed and experiencing an unfortunate decline. This means they are unable to prevent critical disruptions to their operations from a cyber incident and can incur disproportionate impact on their reputation and bottom line as they recover.

Data protection obligations such as those mandated by the California Consumer Privacy Act have been just the beginning of what organizational leadership needs to know.

Are governmental leaders up to speed on new laws governing data protection, including management accountability and notification obligations in the event of a significant cybersecurity incident or data breach? Do they know the right questions to ask IT leads and department heads about systems, safeguards, crisis response plans and staff training, to effectively perform due diligence and maintain regulatory and contractual compliance?

Federal Reporting Requirements

Any organization that deals with federal grant programs or receives federal funding should read up on, and check compliance with, the Federal Information Security Modernization Act (FISMA). FISMA requires agencies to follow NIST cybersecurity standards for risk management and incident response.

The federal Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) impacts state, local and tribal agencies if they operate within designated critical infrastructure sectors. This includes organizations in 16 critical infrastructure sectors (e.g., state run hospitals, public utility authorities, municipal airport authorities or transit agencies). In accordance with CIRCIA, once the final rule goes into effect- cyber incidents must be reported within 72 hours, and ransomware payments must be reported within 24 hours.

Greater Responsibility for State and Local Agencies in 2025

The aim of the March 2025 executive order titled "Achieving Efficiency Through State and Local Preparedness," is to shift more cybersecurity responsibilities to state and local governments, which makes the need for strong and proactive approaches to cyber defense at the state and local level greater than ever. The executive branch's efforts to reduce the federal role in infrastructure cyber resilience will intensify existing cybersecurity weaknesses throughout hospitals, ports, railways and other vital systems, according to industry leaders and cyber experts.

While there is no federal mandate for state and local incident reporting across the board to Cyber Security and Infrastructure Security Agency (CISA) or Department of Homeland Security (DHS), several states now require mandatory incident reporting, with timelines and follow-up requirements aimed at improving cybersecurity coordination and resilience at the local level.

State Cyber Incident Reporting Requirements

Reporting incidents to CISA is currently voluntary for most entities pending final rules. However, all 50 states, the District of Columbia and territories, have their own individual laws with requirements. Here are some examples:

Across individual states, there are many different requirements, approaches and levels of maturity, and the landscape is always changing.

As of 2025, several U.S. states have implemented cyber incident reporting requirements that specifically apply to state and local government agencies. These requirements are often separate from general data breach notification laws and focus on reporting cybersecurity events such as ransomware, unauthorized access, or system disruptions.

California

Requirement: State agencies must report incidents to the California Cybersecurity Integration Center (Cal-CSIC).
Timeline: Immediately upon discovery.
Local governments: Encouraged to report significant incidents.

Colorado

Requirement: State agencies must report incidents to the Office of Information Technology (OIT).
Scope: Includes ransomware, data exfiltration, and system compromise.
Local governments: Encouraged but not always mandated to report.

Florida

Requirement: Florida state agencies must report to the CSOC & FDLE Cybercrime Office.
Timeline: Ransomware: 12 hours; Level 3-5: within 48 hours; Level 1-2; asap.
Local governments: Must report to the CSOC & FDLE Cybercrime Office, Sheriff's Office with jurisdiction.
Timeline: Ransomware: 12 hours; Level 3-5: within 48 hours; Level 1 encouraged, Level 2: mandatory.

New York

Requirement: State agencies must report incidents to the Office of Information Technology Services (ITS).
Local governments: Required to report cybersecurity incidents or ransom demands to New York State Division of Homeland Security and Emerging Services (DHSES)."

North Carolina

Requirement: State agencies must report incidents to the North Carolina Department of Information Technology (NCDIT)
Local Government: Required to incidents that are likely to have a significant impact or meet specific criteria.

Texas

Requirement: State agencies and local governments must report cybersecurity incidents to the Texas Department of Information Resources (DIR).
Timeline: The incident must be reported within 10 days of eradication, closure, and recovery from the incident.

Virginia

Requirement: State and local government entities must report cybersecurity threats and incidents to the Virginia Fusion Intelligence Center.

HIPAA and HITECH

If a state or local agency operates a public health department, Medicaid program, or other healthcare-related service, it may be considered a covered entity or business associate under HIPAA.

The cyber incident implications for agencies must implement administrative, physical, and technical safeguards to protect PHI. If a cyber incident compromises PHI, it may trigger the HIPAA Breach Notification Rule, requiring:

- Notification to affected individuals.
- Notification to the U.S. Department of Health and Human Services (HHS).
- In some cases, notification to the media.

The Health Information Technology for Economic and Clinical Health Act (HITECH) supports HIPAA enforcement and expands breach notification requirements. It encourages adoption of recognized security practices (e.g., NIST frameworks). Agencies that follow these practices may receive reduced penalties in enforcement actions after a breach

Key Takeaways and Next Steps

For mission-driven organizations and their executive leadership, the message is clear: regulators worldwide are making cybersecurity resilience and data protection a priority, so these areas need to be at the top of your agenda as well, now and as the landscape evolves.

The previous section's highlights and resources provide a solid starting point. But your specific cybersecurity and data protection plan will need to check its own legal boxes.

Our Advice:

- See where your own organization stands in terms of the data it collects, the digital systems that bring your mission to life and how everything is protected.
- Identify your strengths, weaknesses, opportunities and threats.
- Keep current with evolving risks, emerging technologies and governance best practices.
- Assess your boards or executive leadership's cyber knowledge and oversight processes. Are leaders able to ask tech leaders the right questions? Can they synthesize the answers and communicate their findings clearly and succinctly to regulators, funding agency and the public?
- Develop a cyber literacy program for leadership teams, boardrooms, commissions and employees to help build a culture of responsible and ethical use of technology to reduce cyber risks. Check for alignment and compliance with AI governance laws and guidance where the organization operates now and plans to operate in the future.
- Bring in your legal advisor or outside counsel early and hire outside help when you need it.