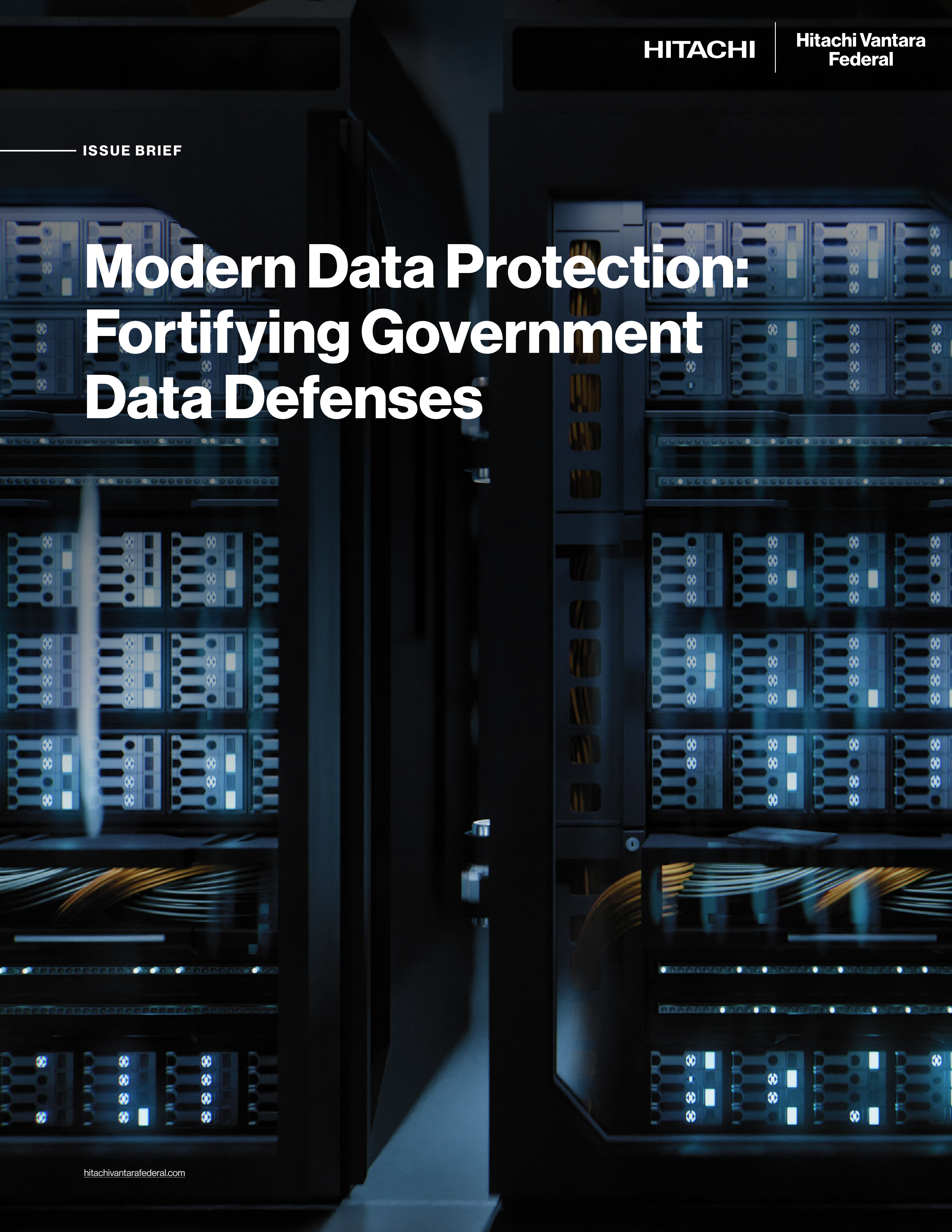


HITACHI | Hitachi Vantara Federal

ISSUE BRIEF

Modern Data Protection: Fortifying Government Data Defenses

hitachivantarafederal.com

Table of Contents

Data is Your Most Strategic Asset, So Why Compromise It?

In a world where technology and threats are always evolving, it's challenging for federal agencies to manage and protect their most strategic resource: data. Data powers government operations and citizen services, yet many agencies are still using legacy approaches to data protection that weren't designed for today's modern infrastructures that span on-premises and the cloud. Outdated technologies create complexity and security vulnerabilities that can put everyone's data at risk.

To protect data and prevent downtime, agencies must be able to rapidly recover from large-scale data loss and protect backups from ransomware. That's why it's time to take a modern, multilayered approach to protect against threats and ensure recoverability when data is impacted.

As Federal IT leaders gear up to address the evolving data landscape, enhancing security and privacy measures stands out as their top 2024 priority.

What are your organization's top data-related priorities for 2024?[1]

#1 Enhancing security and privacy measures

#2 Improving data quality management

#3 Improving speed of data processing

[1] According to The Federal Data Maturity Report: Optimizing Storage, Operations, and Insights, May 2024

Outdated Technology Puts Data at Risk

How can agencies keep up with modern workloads and threats when legacy infrastructures weren't designed to handle today's performance and capacity demands? As data expands and workloads rapidly shift to cloud-native, SaaS and containerized app, cybersecurity becomes more complex and more critical than ever before.

Which applications, if any, do you anticipate will have the most significant impact on your organization's data center needs over the next two years?[1]

#1 Cybersecurity applications

#2 Big data and analytics applications

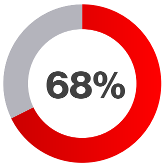
#3 AI/ML applications

#4 IoT applications including sensor data processing

[1] According to The Federal Data Maturity Report: Optimizing Storage, Operations, and Insights, May 2024

Ransomware Is on the Rise

A key factor pushing agencies to address cybersecurity is ransomware. Ransomware attacks are happening more frequently than ever; one study predicts that global ransomware damages will approach $265 billion by 2031. What's most concerning is that these attacks now target the backup that's needed to recover from these incidents. In fact, it's estimated that 90% of ransomware attacks target backups. CIOs and CISOs are making it a priority to mitigate these threats with modern data protection to avoid massive ransom payments, major data loss or both.



of organizations were infected by ransomware in 2021.

The average ransomware payment during 2021 was $570,000.

Executive Orders on Cybersecurity[1]

Executive Orders are placing pressure on agencies to improve cybersecurity by:

- Implementing robust access controls, encryption, automated threat detection, and backup and recovery capabilities to maximize resilience.
- Developing comprehensive incident response plans.
- Fostering a strong data security culture through consistent cybersecurity training.

Which recent executive orders have made the greatest impact on your organizations digital infrastructure priorities? (significant impact)

#1 Executive Order 14028 on improving the Nation's Cybersecurity (47%)

#2 Executive Order 14110 on Safe, Secure, and Trustworthy Development and use of Artificial Intelligence (44%)

#3 Executive Order 14058 on Transforming Federal Customer Experience and Service Delivery to rebuild Trust in Government (37%)

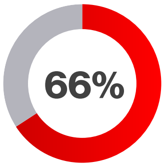
[1] According to The Federal Data Maturity Report: Optimizing Storage, Operations, and Insights, May 2024

Yesterday's Solutions Don't Address Today's Needs

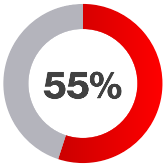
Traditional backup and recovery solutions were not designed to protect today's organizations and IT needs. This is not to say there hasn't been any progress within backup technology: technologies such as virtualization, changed block tracking, and synthetic full backups have moved the needle. But the fact remains: backups take too long to complete. Agencies can't afford the downtime needed to recover from incidents involving multiple systems and large amounts of data.

When backup and recovery can't keep up, agencies may experience a greater dependency on staffing resources, an inability to quickly adopt new technologies, and data silos that prevent them from seeing all their data and acting on it. Also, it can be difficult to meet regulatory requirements and deliver service level agreements.

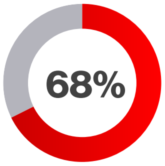
The result is that today's traditional backup and recovery solutions put agencies at greater risk, incurring unnecessary hardware and staffing costs and creating a more complex environment. New threats, combined with large IT environments and vast amounts of data, require new approaches.



of agencies are concerned that their data infrastructure may not be resilient enough to recover all data if they were faced with a ransomware attack.



of Federal IT leaders share concerns that their organization may not be able to detect a data breach in time to protect data.



of organizations were infected by ransomware in 2021, with an average ransomware payment of $570,000.

What Are Traditional Backup and Recovery Solutions?

Many agencies still use tapes for backups, which have been around for ages. This solution is inefficient: data is backed up to tape, and then those tapes are shipped offsite for safekeeping. Organizations have to physically locate and then transport the tapes back to the premises in order to recover data.

Not only are tapes time consuming to manage, but they are also plagued with hardware compatibility issues and have very limited durability. Over time, tapes result in poor recovery performance or they just fail altogether. There is also a risk of overwriting the data needed to recover from an outage or malicious attack.

Today it's unrealistic to backup and restore petabytes of data with tapes on a regular basis with any kind of reliability, especially if organizations are trying to sustain positive uptime and data availability KPIs.

Tape Storage Issues

Subject to media failure/loss

50% of tape restores fail

Time consuming to manage

Slow backups and restores

It’s Time to Evolve to a Modern Data Protection and Cyber Resiliency Approach

It’s risky for agencies to rely only on backup and recovery to maintain continuity of operations and recover from cyber attacks. If data needs to be suddenly recovered after an unexpected incident, would the nightly backup-to-tape be enough to restore it all? True operational resilience requires a modern approach.

What Is Modern Data Protection?

Modern data protection is a combination of strategies, technologies and best practices to protect data across various platforms, including on-premises, cloud and hybrid environments. This integrated approach leverages advanced technologies like artificial intelligence (AI), machine learning (ML), and automation to enhance data protection capabilities and ensure robust defense against evolving threats.

Key Components of Modern Data Protection:

1. **Data Backup and Recovery:** Regularly creating copies of data to ensure it can be restored in the event of loss, corruption, or disaster. This includes traditional backups as well as more advanced solutions like continuous data protection (CDP).

2. **Disaster Recovery:** Implementing plans and systems to quickly recover and restore data and applications after a catastrophic event, minimizing downtime and data loss.

3. **Data Archiving:** Storing long-term data in a way that it remains accessible and secure, often for compliance or regulatory purposes.

4. **Data Management:** Organizing, storing, and managing data efficiently to ensure it remains protected and available when needed.

5. **Cloud Data Protection:** Extending data protection strategies to include data stored and processed in cloud environments, ensuring that cloud-based data is as secure as on-premises data.

6. **Ransomware Protection:** Implementing measures to detect, prevent, and recover from ransomware attacks, which are increasingly targeting organizations’ critical data.

7. **Data Governance:** Establishing policies and procedures to manage the availability, usability, integrity, and security of data used in an organization.

What To Expect from the Right Modern Data Protection Solution

The main goal of modern data protection is to reduce the risk of losing valuable data—but there's more to gain from the right solution. What should an agency expect from modern data protection?

Simplified Management

Get a consistent view of backups across various workloads in the hybrid cloud to reduce internal overheads and simplify the management of backups and recovery.

Faster Backup and Recovery

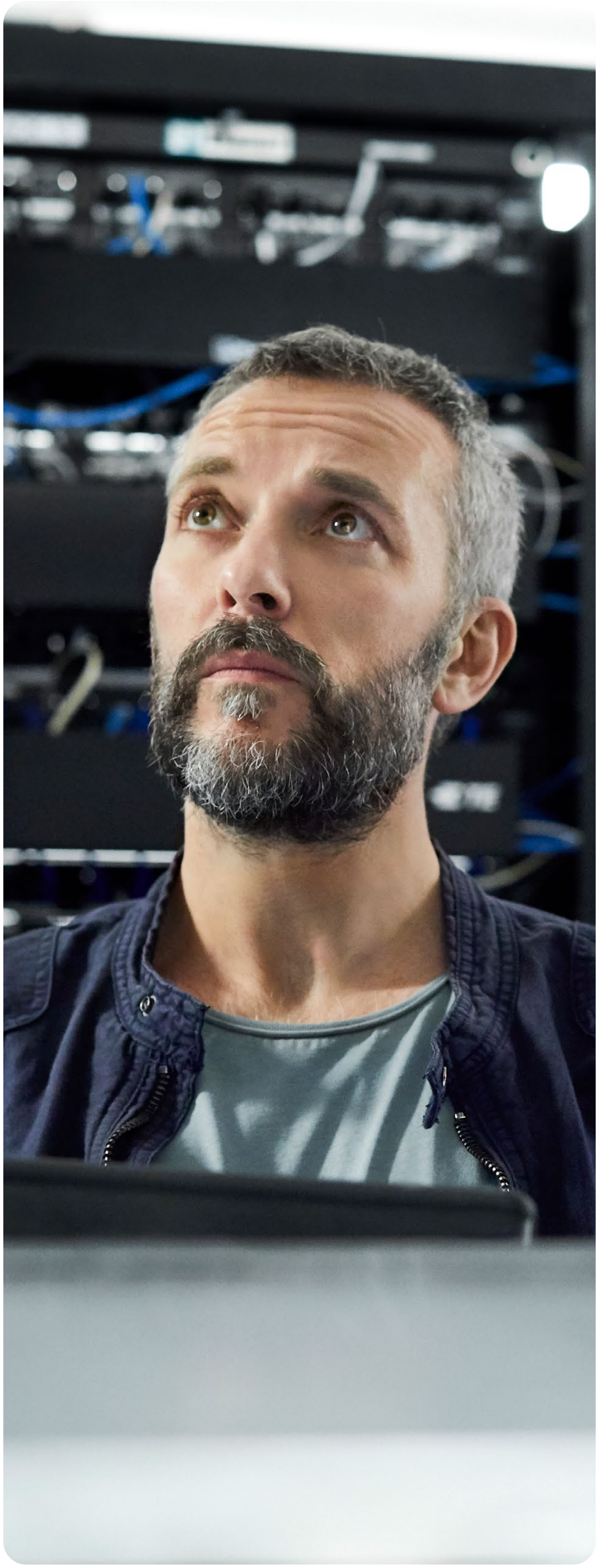
Improve the speed of recovery to be as close to the present as possible with infrastructure that features advanced AI/ML technologies and automation.

Mitigation for Ransomware or Cyberattacks

Safeguard critical information in the event of a ransomware attack by detecting malware/ransomware quickly and isolating systems as soon as possible.

Reduction of Costs

Manage more data with fewer resources to reduce the cost of long-term data retention. No more rooms full of tapes to ship, store and sort.



Get Modern Data Protection with Hitachi Vantara Federal

Implement the key components of modern data protection with Hitachi Vantara Federal and its reliable, secure, immutable infrastructure including the 100% availability guarantee of Virtual Storage Platform (VSP) One and the 15 nines of data durability and 10 nines of data accessibility of the Hitachi Content Platform (HCP).

Availability

Ensure continuous operations for mission critical applications with nonstop, uninterrupted data access to achieve strict zero RTO and RPO objectives.

Virtual Storage Platform (VSP) One

The Hitachi Virtual Storage Platform One offers an industry-first 100% Data Availability Guarantee that has supported the world's most diverse and challenging open systems and mainframe databases and applications for more than two decades.

Backup

Deliver robust protection of data where it lives to reduce the cost of traditional data protection and reduce the risk of data loss.

VSP One, HCP

Simplify backups to cloud (object) with HCP backed by VSP One storage as a tape/cloud SaaS alternative. Protect these backups with data protection software tools like Hitachi Ops Center Protector and key ISV partners like Commvault, Veritas and Veeam.

Recovery

Quickly recover from system failures, user errors and malicious attacks.

Ops Center Protector, DPaaS, Hitachi Data Protection Suite, CyberVR

Hitachi Vantara Federal offers the world's fastest automated ransomware recovery. Ops Center Protector together with CyberVR are capable of handling recovery of more than 1,500 VMs with over 100 TB of data allowing production to resume fully protected all in 70 minutes.

Protection

Protect data at the edge from ransomware and other threats and quickly restore backups when inevitable attacks happen.

Commvault HyperScale X combined with Hitachi HCP Cloud Scale

Hitachi Data Protection Suite (HDPS), powered by Commvault, delivers a unified, modern offering that facilitates the backup, recovery and management of enterprise and application data.

HCP Anywhere Enterprise

HCP Anywhere Enterprise powered by CTERA offers continuous real-time protection at the edge,synchronizing the data to air-gapped, immutable object storage. This provides a superior defense against ransomware attacks, with RPO (recovery point objective) measured in minutes or seconds, compared to traditional backup products for endpoints and servers that typically back up data every 8 to 24 hours.

Is Your Agency Ready for Modern Data Protection?

If you're like most agencies, you're finding it challenging to ensure critical information is protected from the risk of application failure or cyber compromise, especially when IT staff is overwhelmed by data complexity, workloads and managing backup and recovery using hybrid cloud. That's why it's the right time to make a move to modern data protection—there's no need to wait for an incident to initiate change.

Hitachi Vantara Federal makes it easy to adopt modern data protection due to the ease of configuration, management and reduced overheads with Commvault Cloud. In fact, you'll only need one person assigned to the transition process to get started. With unlimited cloud storage and retention, you'll be free from unreliable tape backups and offsite storage components, saving hardware costs and management overheads. On the operations side, your team will be able to respond quickly to compliance requests with the same indexing capability as the past on-premises Commvault solution.

So, what are you waiting for? Let's discuss your backup strategy today.

ABOUT HITACHI VANTARA FEDERAL

Hitachi Vantara Federal is the trusted leader in mission-centric data solutions for the Federal government. We're a collaborative, full-service company with longstanding OT/IT roots. We empower data-driven insight with a deep bench of integrated partners — advancing Federal customer missions regardless of their data maturity levels. Hitachi Vantara Federal is a FOCI-mitigated subsidiary of Hitachi Vantara. Visit us at hitachivantarafederal.com.

To learn more, visit:

hitachivantarafederal.com →

Hitachi Vantara Federal

Corporate Headquarters
11950 Democracy Drive, Suite 200
Reston, VA 20190 USA
hitachivantarafederal.com

Contact Information
info@hitachivantarafederal.com
hitachivantarafederal.com/contact-us/