*White paper*

# Enabling Seamless Tech Consolidation and Cross Agency Access for Federated *Federal Agencies*

## The Federal Technology Consolidation Landscape

Federal agencies operating in a federated model each maintain unique IT systems, processes, and security policies—resulting in siloed operations and redundant spending. Recent mandates drive the need to consolidate technology platforms and budgets to a central headquarters, aiming for increased efficiency, stronger cybersecurity, and simplified user experience. Such transitions, however, introduce significant technical, operational, and human challenges, mirroring many of the complexities found in mergers and acquisitions (M&A) transactions, including:

- Integrating diverse systems and applications without disrupting ongoing agency missions.
- Ensuring compliance with agency-specific regulations and federal cybersecurity mandates.
- Maintaining user productivity and morale throughout the transition.
- Minimizing attack surfaces during periods of organizational and technological change.

This paper focuses on the critical “day one” experience for employees who need access to new applications and resources on the day consolidation is finalized.

## Traditional Approaches: Obstacles to Success

No two technical consolidations are exactly the same, as each agency brings its own unique combination of technologies and workflows. Complicating factors like regional data regulations, regulatory compliance, or highly sensitive intellectual property add to the challenge. There’s often a tension between the desire for a fast and efficient merger of the two organizations and the need for gradual migrations to uphold robust security and operational standards. While far from exhaustive, the sections below describe three common approaches to “day one” onboarding as part of a technology consolidation.

Past technology consolidation efforts have typically relied on one of three approaches, each with clear limitations:

### Do Nothing

Maintain existing IT silos and merely connect back-end systems. This fails to achieve operational efficiency, keeps agencies isolated, and complicates cross-agency workflows and reporting.

In some situations, it may be possible to “do nothing” (or very little) with regards to the employee endpoints while connecting back-end IT systems. This might be appropriate for smaller organizations with a distributed workforce who are and using software-as-a-service (SaaS) apps for most workflows. This approach would not fit well for organizations with strong cybersecurity practices or any kind of regulatory compliance requirements.

### Ship New Hardware

A common approach would be to replace all agency devices with HQ-provisioned laptops and accounts like the regular onboarding playbook—the, same as for new hires.

This typically means creating a new set of credentials and accounts, then issuing a new laptop and other necessary hardware. There's a natural advantage to using the same tried- and- true method for onboarding, reducing the likelihood of unexpected issues.

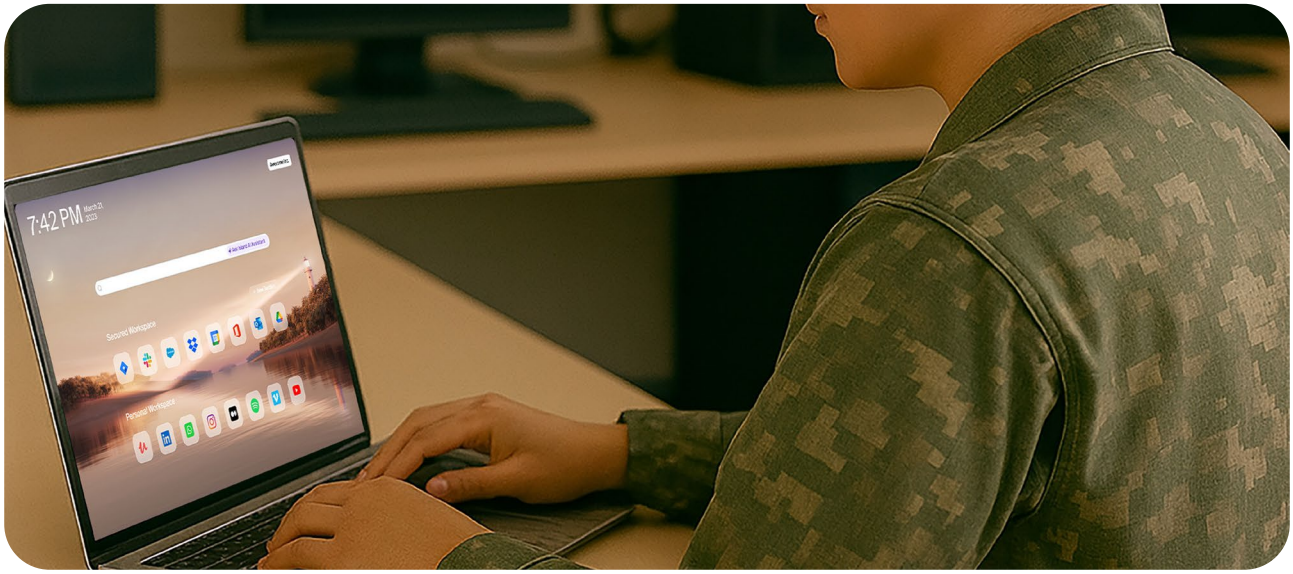
The downside to this approach is twofold: first, it adds significant operational and logistical demands on the IT organization. With small agencies this may not matter but for large organizations with thousands of employees the costs are significant. The larger cost, while harder to measure, is the added friction on the employees who need to juggle their work between two laptops, two email inboxes, two sets of files. Employees often experience a sense of uncertainty about their place in the newly consolidated organization, and making their day-to- day workspace less productive only adds to that discomfort.

### Provision Virtual Desktops

Provide access to HQ environments via virtual desktops, reducing hardware logistics but introducing friction, complexity, and high infrastructure costs.

A refinement of shipping laptops is to set up a virtual desktop that users can access from their existing laptop. This approach reduces the logistical challenge of configuring and shipping thousands of laptops, but that benefit doesn't come for free. A virtual desktop adds friction for employees who need to jump between their regular desktop and virtual desktop depending on the task. It may be marginally easier than swapping between two physical laptops, but in practice it's still a poor user experience. For the IT organization, any savings from avoiding laptop provisioning are consumed by increased costs and operational complexity of virtualization infrastructure.

Each approach exposes agencies to cybersecurity risks, impedes mission continuity, and can drain both time and resources.



## A New Approach

Island, the Enterprise Browser, offers a new approach for federated IT consolidation, communication and access that eliminates all the points of friction outlined above, while maintaining robust security and access controls. With Island, the consolidation experience looks something like this:
On day one, employees are encouraged to launch Island and login with their new credentials. They're greeted with a personalized message welcoming them to their federal workspace and directing them to the handful of key applications they need to complete their onboarding process. From day one onward, Island is their workspace for accessing critical applications and resources. As a browser, the experience is intuitive and familiar. Internal applications are easily accessed, without the need to juggle VPN client connections. Over time, more applications are added to their personalized home screen as the IT teams complete each migration or consolidation project.
The employee experience is the most visible part of the communication, access and consolidation experience, but Island offers real advantages for IT and Security teams as well

### Simplified Deployment and Management

Island can be rapidly deployed using existing federal endpoint management tools or through user self-installation. IT teams can preconfigure access to headquarters resources based on role, agency, or location. Additionally, real-time dashboards track onboarding progress and browser usage, enabling immediate support and ensuring successful adoption

### Application access

In preparation for day one, IT teams can configure Island to make important applications available to the users based on their role, location, or other criteria. Most applications will use single sign-on from an identity provider (IDP), but Island offers flexibility with integrated privileged access management and enterprise password manager for applications that aren't SSO enabled.

### Network connectivity

For organizations that use privately hosted applications, network access is a critical component for day- one access. Island offers integrated zero trust network access (ZTNA) to securely connect to internal networks without the need for a VPN. Along with
application access, IT teams can configure the network access ahead of time so there's no friction on day one.

### Adoption metrics

By using Island for onboarding, IT teams gain real-time metrics to gauge adoption. As users login to Island on day one, dashboards in the Island Management Console track usage by group or location. This is particularly valuable for distributed organizations and offers fast feedback to identify and resolve any issues in onboarding.

### Day-One Productivity and Security

Users can continue using their existing endpoints by simply installing Island and authenticating with their headquarters-assigned credentials. Once logged in, employees gain immediate access to critical headquarters applications through a secure, familiar browser interface, eliminating the need to manage hardware, virtual desktop infrastructure (VDI) sessions, or multiple user profiles. Personalized onboarding messages and resource hubs welcome users on their first day, reducing confusion and ensuring a smooth, seamless transition.

### Compliance and Security Built-In

Island supports granular access controls, integrates with federal-standard identity providers, and enforces ZTNA. Its privileged access management capabilities ensure secure handling of applications that have not yet been migrated to headquarters SSO. In addition, security teams can enforce data residency and protection mandates, enabling compliance with evolving federal requirements

### Lower Cost, Higher Efficiency

The Island Enterprise Browser enables federated federal agencies to consolidate technology at headquarters quickly, securely, and without costly hardware replacements or complex VDI setups. Deployed to existing devices, it gives employees immediate, secure access to HQ applications through a familiar browser, while IT manages granular access, compliance, and real-time adoption metrics. By reducing friction, cutting costs, and providing reusable onboarding playbooks, Island supports smooth integration, future agency onboarding, and secure offboarding—all with minimal disruption to mission-critical work.

## Why Island for Federal Agency Consolidation?

Island uniquely addresses federal needs for security, compliance, agility, and user experience—making it the optimal workspace for both day-one onboarding and longer-term operational efficiency as federal agencies consolidate technology at scale.

Learn more about how Island supports smooth, secure, and cost-effective federal technology transformation at www.island.io/industries/government