IRON MOUNTAIN®

GOVERNMENT SOLUTIONS

WHITE PAPER

IT ASSET DISPOSITION THE RIGHT WAY: PREVENT A DATA BREACH

CONTENTS

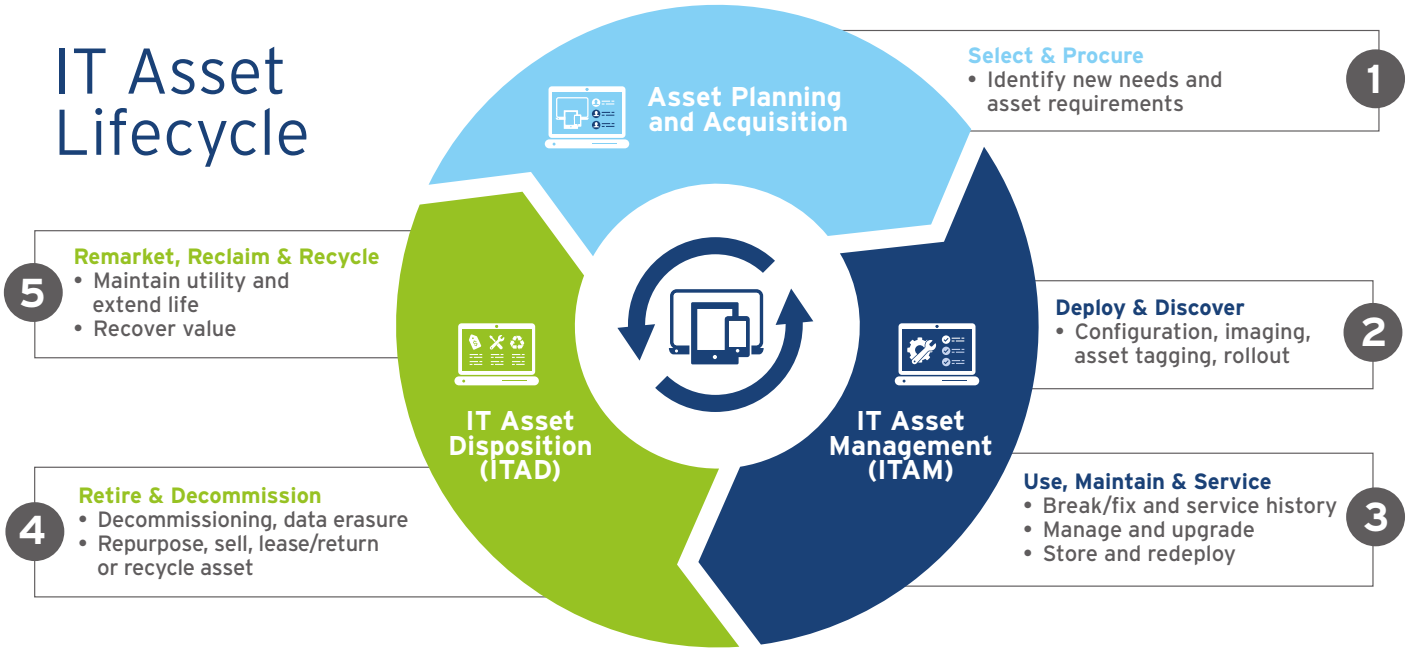
GROWTH IN ELECTRONIC DATA AND TECHNOLOGY MODERNIZATION

The technology that creates, enables, and communicates the growth in electronic data, continues to proliferate at an exponential pace. In order to evolve with this growth, while working to achieve their missions, government agencies are following trends and adopting new technologies, especially those that are data-bearing assets - laptops, PCs, servers, printers and mobile devices.

As devices become outdated or reach the end of their useful life, agencies need to ensure that each individual asset is taken care of in a secure and sustainable way.

Given the security, privacy, and environmental concerns associated with the retiring of IT assets, agencies must ensure they are taken care of in a responsible manner and in adherence to government regulations. A comprehensive IT Asset Disposition (ITAD) program needs to be part of every agency's overall data management strategy.

Disposing of obsolete assets in a manner that is legal, safe, cost-effective, and free of institutional harm is a challenge for all government agencies. Achieving ITAD success requires navigating legal and regulatory requirements, including NIST 800-88 standards, DoD 5200.22-M data sanitation requirements, HIPAA/ HITECH, and Federal Assets Sale Transfer Act (FASTA) mandates. Poorly executed disposition of IT assets can result in fines, public health and safety issues, breaches in data security, and reputational harm.

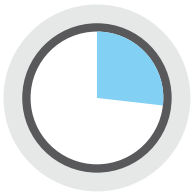


Nearly half of Federal Government respondents in a Thales Data Threat Report noted they have experienced a security breach at some point, and of these, 47% said they had experienced a breach in the last 12 months. Most agencies do not have a solid understanding about what data they have or where it is located. Just over one-fourth (28%) of federal respondents have full knowledge of where their data is stored, and just one-third (33%) claimed to be able to fully classify their data. This means that personal and sensitive data can be anywhere, including on technology assets that are no longer in use – putting agencies at enormous risk and with multiple challenges to mitigate that risk.

NEARLY 50%

noted they have experienced a security breach at some point

ONLY 28%



of Federal Government respondents fully know where their data is located

JUST 33%

are able to fully classify their data

Source: Global Industry Analysts

GOVERNMENT FOCUS ON DATA PROTECTION

The Federal Government has recognized the need to dedicate funding to address these urgent IT modernization challenges. The Technology Modernization Fund (TMF) aims to secure government sensitive systems and data, with the purpose to "fund projects for technology-related activities to improve information technology and to enhance cybersecurity across the Federal Government." To date, the TMF has received $175 million through the annual budget process and $1 billion through the American Rescue Plan. A two-phased proposal process allows federal organizations to apply for funding to address immediate security gaps, such as disposing of data-bearing IT assets.

Additionally, the Senate Homeland Security and Governmental Affairs Committee approved legislation to advance the federal government's technology modernization efforts. Know as the Legacy IT Reduction Act, the bill will require agencies to develop an inventory of legacy IT systems as well as write modernization plans to update or dispose of those systems. The Act reinforces a longstanding federal data privacy and security requirement across the information management lifecycle and it provides a pathway to eliminate old IT equipment that runs much of the government today.

> "The Federal Government must bring to bear the full scope of its authorities and resources to protect and secure its computer systems, whether they are cloud-based, on-premises, or hybrid. The scope of protection and security must include systems that process data (information technology (IT) and those that run the vital machinery that ensures our safety (operational technology (OT))."
>
> – Executive Order on Improving the Nation's Cybersecurity

SECURING INFORMATION WITH TECHNOLOGY DISPOSITION

Federal agencies are progressing in transitioning to a digital-first environment. This environment is evolving quickly due to the nature of technology proliferation. IT departments must remain ahead of the curve and can look to the following use cases to take a proactive approach.

DATA CENTERS

As cloud migration continues to increase, the reliance on government-housed data centers will become obsolete, requiring appropriate disposition of equipment. The COVID-19 pandemic has only accelerated this focus, with total federal cloud spending greater than $8B, according to **Bloomberg Government statistics and Deloitte analysis.** This trend will enable agencies to transition away from on-premises data center equipment, providing an opportunity to significantly consolidate the technology required in these environments leading to a significant volume of excess IT equipment.

OFFICE SPACE

The Reduce the Footprint policy issued by the Office of Management and Budget (OMB) requires agencies to move aggressively to dispose of surplus properties held by the federal government, make more efficient use of the government's real property assets and reduce the total square footage of their offices. In November 2021, General Services Administration (GSA) Administrator Robin Carnahan told members of the House Transportation and Infrastructure Committee that 40% of its leases would expire over the next four years. The closing of offices and government buildings will require a strong look and assessment of the legacy technology equipment resulting in a significant opportunity to securely dispose of legacy assets.

HYBRID WORKERS

The hybrid workforce is expected to continue. Federal agencies will need to support the remote workforce with new or refreshed devices, disposing of the traditional in-office technology such as desktops, storage drives, printers and more.

INTELLECTUAL PROPERTY

Legacy hardware that stores intellectual property (IP), such as health-related research, geospatial data, contractual information, and patent/trademark applications are other candidates for secure ITAD. This technology must be securely removed, transported, and destroyed to ensure any IP information is wiped following strict guidelines.

ENVIRONMENTAL, SOCIAL AND GOVERNANCE

Agencies need innovative solutions that bring them closer to achieving their Environmental, Social and Governance (ESG) goals. Environmental solutions, in particular, allow the recycling process for technology assets to reduce greenhouse gas emissions, cut pollution and save energy and resources to improve green posture.

For every million cell phones recycled, the following can be recovered:

35,000
pounds of copper

772
pounds of silver

75
pounds of gold

33
pounds of palladium

Globally, only 9.7M tons of IT waste is recycled or remarketed annually (20%)

Recycling one million laptops saves the energy equivalent to the electricity used by more than 3,500 US homes in one year.

A STRUCTURED APPROACH TO DISPOSITION

Outsourcing an ITAD program to an industry-leading third-party vendor with expertise in disposal can expedite the entire process and serve as a more economical use of agency resources. Agencies have traditionally performed ITAD as point-in-time projects, which come at higher prices than an established program. Third-party disposition of assets is cost-effective due to economies of scale, and can help long-term budgeting. Additionally, a comprehensive program can result in avoidance of fines and other costs associated with mismanaged ITAD.

A proper program should be viewed as a data security and environmental sustainability investment that adheres to a structured approach.

1. **Identifying sensitive data.** Understand which agency assets contain sensitive data and where these key assets are located.

2. **Establishing policies and procedures.** Implement consistent programs throughout the organization and monitor for compliance. It is crucial all employees are aware and understand the policies and procedures.

3. **Focusing on secure chain of custody.** Rather than a one-size-fits-all approach to processes and data sanitization methods, focus on security tailored to the nature of the data that includes tracking mechanisms to follow an asset from pick-up to destruction.

When an agency deploys a comprehensive disposition process and program, with a qualified third-party vendor, they can mitigate many concerns that can currently exist.

THE DANGERS OF IMPROPER ITAD

When federal organizations determine the need and secure the funding for ITAD, the first phase to moving forward in the disposition process is to consider several concerns from both an agency and third-party vendor perspective.

Negligence. It is both costly and time consuming to destroy data bearing IT assets, which provides an unfortunate opportunity of not adhering to regulations when disposing of IT equipment.

Human error. Internal employees or ITAD service providers cannot tell if data was properly sanitized simply by looking at the media on which it resides.

Improper handling. If the chain of custody is not verifiable, there is no way of knowing for sure whether equipment was diverted to a secondary market, landfill or elsewhere.

Environmental damage. If retired IT assets are not properly handled in an environmentally compliant manner, the agency faces incremental risk for fines, penalties and possible reputational harm. Focusing on meeting sustainability goals cost-effectively allows equipment to be managed in ways that reduce greenhouse gas emissions, cut pollution and save energy and resources.

By evaluating a strategic partner and ensuring a proper ITAD program is in place, federal agencies will be able to avoid the dangers and pitfalls of improper disposition.

MAXIMIZE PROTECTION AND VALUE

Proper evaluation of a strategic partner is critical to maximizing protection, compliance and value to federal organizations. Look for partners who comply with all regulations, industry best practices, and will legitimately dispose of IT assets. The onus to ensure data protection and environmental recycling practices ultimately falls to the government agency.

MANAGE RETIRED IT EQUIPMENT

Disposition processes must be highly regimented and consistent. Agencies should have access to alternative destruction methods and locations: bulk or serialized media destruction and on-site or off-site destruction capabilities. Some organizations, such as defense or federal healthcare institutions, might not want any data-bearing devices to leave the premises – thus requiring an on-site data destruction solution.

AUDITABLE PROCESS AND WORKFLOW

Each item marked for disposal should be logged in an inventory and tracked through the entire disposal process. A best practice is to affix a scan code at the point of surrender and scan the tag at each hand-off point, allowing an agency to audit the process at any time. The inventory management system should flag any missing items and create an exception report.

SECURE LOGISTICS, TRANSPORTATION AND VEHICLES

Equipment is never more vulnerable than when it's in transit. Items can fall off open truck beds, and unlocked vans are an invitation to thieves. Look for ITAD providers that use closed, secured transportation and secure handoff points monitored by closed-circuit cameras.

PROOF OR CERTIFICATION OF DESTRUCTION

This is a document that verifies equipment has been scrubbed, recycled or destroyed in a manner that satisfies the terms of the contract. It's best to work with an ITAD vendor that has been certified by a respected third-party standards organization such as e-Stewards or Sustainable Electronics Recycling International.

COMPLIANT, ENVIRONMENTALLY SENSITIVE DISPOSAL

The provider should guarantee all IT assets are disposed of in an environmentally friendly manner that meets local, state and federal requirements. The provider's operations should adhere to widely recognized certification standards established by credible industry organizations, such as e-Stewards, R2 and RIOS.

CONCLUSION

With the continued growth of technology, disposing of devices securely and in a sustainable way is a priority for federal agencies. When transitioning to a digital-first environment, it is critical for agencies to protect their data and avoid the risk of a data breach. By having a comprehensive ITAD program, agencies can have insight on the status and security of all assets being disposed.

Working with a reputable third-party vendor to customize a comprehensive and secure ITAD strategy and program can reduce your risk and possibility of data loss by leveraging their experience and best practices. by investing the time and effort to create and enterprise program, agencies can help safeguard their IT assets and the data that is entrusted to them.

To talk to an ITAD representative of Iron Mountain Government Solutions, email **publicsector@ironmountain.com.**

IRON MOUNTAIN®

GOVERNMENT SOLUTIONS

ABOUT IRON MOUNTAIN

Iron Mountain Incorporated (NYSE: IRM) is the global leader in innovative storage and information management services, storing and protecting billions of valued assets, including critical business information, highly sensitive data, and cultural and historical artifacts. Founded in 1951 and trusted by more than 225,000 customers worldwide, Iron Mountain helps customers CLIMB HIGHER™ to transform their businesses. We provide services to state and local government and educational agencies to assist with enhancing the data privacy and security of your citizens. Visit www.ironmountain.com for more information.

ITRenew:
Iron Mountain offers a "one stop shop" for ITAD with the acquisition of ITRenew. Combining ITRenew's ITAD software and services with Iron Mountain's secure chain of custody and logistics, government agencies can safely and securely dispose of their IT assets, including PCs and laptops, servers, hard drives and mobile devices, with the peace of mind that disposal complies with applicable data security and e-waste disposal regulations.

USFED-ITAD WHITEPAPER-111423