ivanti

Simplifying CDM and FISMA reporting requirements with Ivanti

Table of Contents

Executive Summary

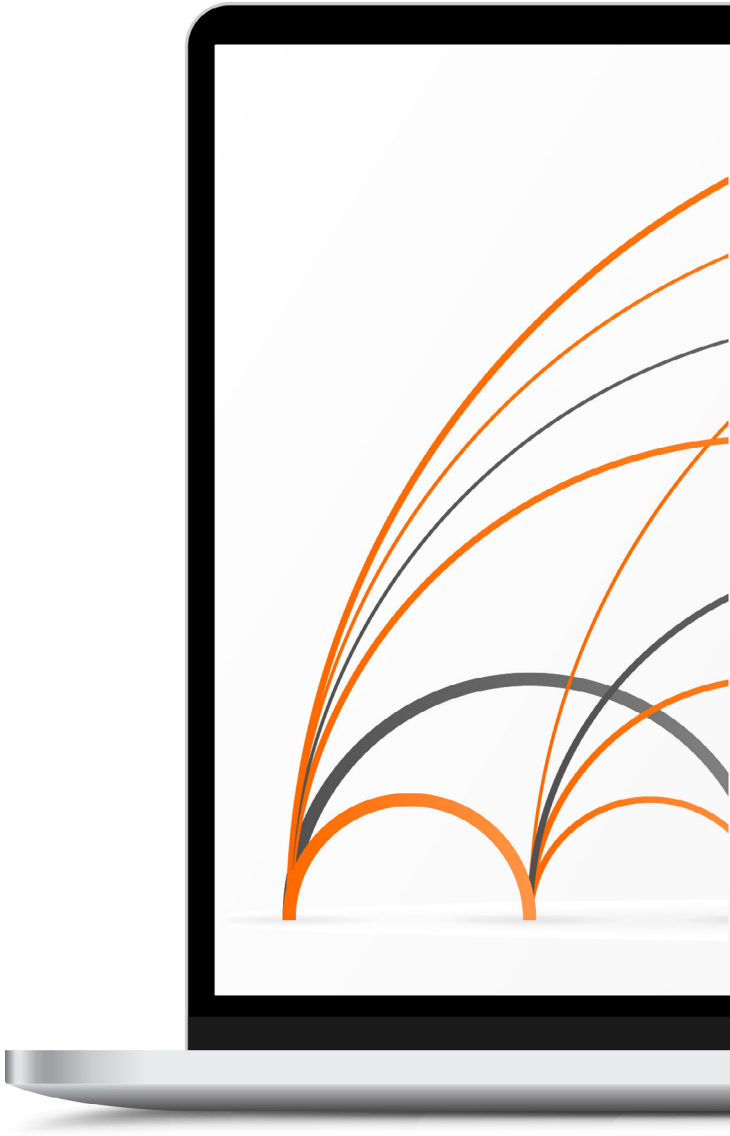
Today's emerging workforce in the United States does not know a world before mobile devices. Nearly all Americans (96%) own some type of cell phone and most of those are smartphones (81%). Most of today's workforce owns multiple mobile devices and uses them interchangeably for both personal and professional tasks. For many federal employees and contractors, the term "mobile device" includes not only smartphones (iOS, Android, etc.) but also modern tablets and laptops that run macOS or Windows 10. Collectively these devices are known as the "modern mobile endpoint." Throughout this paper we will refer to mobile devices, which applies to all modern mobile endpoints including smartphones, smartwatches, tablets, laptops, desktops, and more.

One of the biggest challenges with securing these devices is the fact they are always on and always connected, often to both the Internet and the agency's enterprise network. This constant connectivity, if left unmanaged and unsecured, can put government and enterprise applications and data at risk. This means federal agencies need to rethink how they approach mobile security, because mobile devices are now part of the agency's network and need to be managed with the same security controls enforced on the enterprise network and across the agency's IT infrastructure and staff.

To help agencies better protect against cyberthreats, the Continuous Diagnostics and Mitigation (CDM) program was formed to help agencies improve reporting, information sharing and implement stronger controls to protect agencies' networks, data, and resources.

The CDM program has matured since its initial implementation, but overall it focuses on helping agencies to understand who and what is on the network, what is happening on the network, and how to protect the agency's data and applications. Ivanti, a leading provider of Unified Endpoint Management (UEM), is uniquely capable of supporting the goals of the CDM program. With a comprehensive UEM platform, federal agencies can better protect their resources, applications, and data while increasing security and visibility across their entire mobile infrastructure.

Ivanti helps federal agencies enable secure mobile productivity by greatly simplifying the mobile security experience for both IT and the end user. Our mobile-centric, zero trust platform enables federal agencies to ensure that only trusted devices, users, apps, networks, and applications can access government resources. As a result, Ivanti makes it easier for agencies to comply with the CDM and FISMA reporting requirements.



1 Pew Research, "Demographics of Mobile Device Ownership and Adoption in the United States," June 2019.

2 Note: Throughout this document, Mobile Device Management (MDM), Enterprise Mobility Management (EMM) and Unified Endpoint Management (UEM) are synonymous. Generally, the market analysts have adopted UEM as a replacement term for the traditional terms MDM and EMM.

Why Mobile Security is Critical to CDM

Since 2011, mobile traffic has increased by more than 222%. Today, more than 50% of worldwide Internet traffic is from mobile devices. As 5G gains more traction, there will likely be a significant uptick in mobile traffic again, growing exponentially over the next five years.

Many federal agencies are already taking advantage of new platforms and embracing digital transformation to deliver a better user experience and improve access to government services (especially citizen-facing services). For instance, many agencies are launching innovative initiatives for microservices, moving more services to the cloud, and developing new mobile apps. However, the associated risk accompanying this transformation is that devices directly accessing these microservices typically bypass the enterprise security controls and network protections traditionally relied upon to secure the enterprise.

Here's why: Modern endpoints are often allowed to simultaneously connect to both the government enterprise network and the Internet. This split-tunneling approach can compromise the security of federal enterprise resources, which may be subject to cyberthreats launched through untrusted public Wi-Fi or home networks. In addition to split-tunneling, the modern endpoint greatly expands the threat surface for cyber attacks. Devices outside of the control of the agency's IT professionals could not be imagined and would not be allowed by cybersecurity and risk policies just a few years ago, but are now commonplace and frequently overlooked.

The era of COVID-19 is compounding these challenges by greatly expanding the threat landscape in an extremely short time period. Working from home (telework) has become the new normal, and many agencies have had to hastily enact teleworking policies nearly overnight and with very little planning. As a result, federal agencies have many more employees and contractors remotely accessing resources on their enterprise networks than ever before, including workers (both employees and contractors) who were not previously approved for telework. These users are now empowered to work from home to ensure critical projects don't fall behind schedule, for the good of the mission. This has been enabled and reinforced by memos from the Office of Management and Budget recommending, to the fullest extent possible, flexibility and allowance for telework and user access. (See OMB M 20-15 and OMB 20-18 for more information.)

> "We're about to begin an effort to work with agencies to pull in their mobile asset data from their enterprise mobility management systems. So we're venturing in on the mobile side"
>
> **Kevin Cox**
> Read the full article

The challenges resulting from the rapid adoption of teleworking may include a lack of effective and consistently enforced security controls. For example, VPN capacity in many agencies was neither sufficient nor properly configured for the flood of concurrent VPN sessions. In many cases, the network VPN provides little additional security when the encrypted session terminates at the network perimeter. The surge of remote connections to federal resources from potentially unknown and unmanaged personal devices has resulted in a lack of available VPN capacity and increased latency from "hairpinning." This occurs when devices outside of the enterprise access resources that are also outside of the enterprise. And yet, the traditional VPN forces the traffic to be routed to the enterprise through the VPN server on the network, and then back out to the externally addressable target. This creates additional volume and load on the enterprise VPN when it would be more efficient to directly connect to the external resource from the external device. This more efficient solution, however, needs to have appropriate controls in place, since it will bypass the perimeter VPN solution.

3 Broadband Search, "Mobile vs. Desktop Usage (Latest 2020 Data), BroadbandSearch.net

NIST Recommendations

A critical aspect of an agency's cybersecurity posture is the management of mobile devices that access the enterprise network and resources. The proliferation of mobile devices expands the agency's threat surface and should only be permitted with effective threat detection, remediation, and compensating security and privacy controls. The NIST DRAFT Special Publication 800-124 Rev 2 specifically recommends that "Organizations should employ Enterprise Mobility Management, Mobile Threat Defense, and other applicable enterprise mobile security technologies." DHS and CISA have gone one step further, recommending that UEM, Mobile Threat Defense, and application vetting all be deployed by federal agencies, and that they be deployed as a unified solution and not separate stove-pipe solutions.

An effective threat defense solution supports configurable on-device detection and automated remediation of mobile threats. The software should detect and self-remediate threats at the device, network, and application level. Additionally, it should provide phishing protection in mobile email, SMS, chat apps, and other on-device conversational mechanisms. A solution should offer tiered compliance actions, configurable responses to include alerting an end user, and more significant actions that include retirement and/or an automatic device wipe.

UEM solutions should enable an agency to enforce access control by making a user's phone a policy enforcement point (PEP) for the agency. This helps support the agency's zero trust strategy for authorization decisions. The disintegration of the traditional strong network perimeter is a result of Wi-Fi, cellular, and always on/always connected devices that connect from anywhere, on any network. To enable a secure, perimeterless agency, IT needs to provide effective secure access to applications and data through a frictionless user experience that is seamlessly enabled on any device, whether owned by the employee or the agency.

The National Institute for Standards and Technology (NIST) Special Publications 800-124 Rev 2 (Draft) actually addresses the reality of today's modern mobile government agency in its "Guidelines for Managing the Security of Mobile Devices in the Enterprise." As stated in the NIST report, "Mobile devices were initially personal consumer communication devices, but they are now permanent fixtures in enterprises and are used to access modern networks and systems to process sensitive data."

4 NIST, "Guidelines for Managing the Security of Mobile Devices in the Enterprise," March 2020. https://csrc.nist.gov/publications/detail/sp/800-124/rev-2/draft

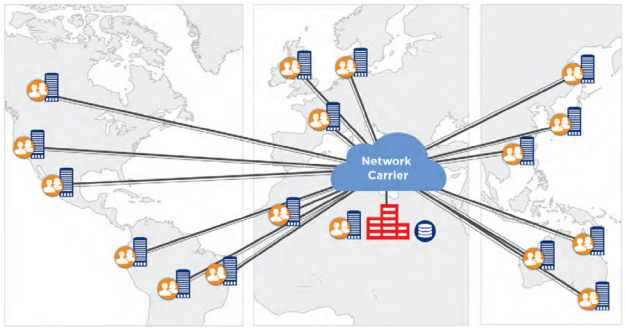
5 DHS.gov, "News Release: DHS S&T Study Recommends Federal Agencies Integrate EMM & APP Vetting Solutions for Maximum Security," Aug. 2019. https://www.dhs.gov/science-and-technology/news/2019/08/27/news-release-dhsst-recommends-integration-emm-app

Telework and BYOD

In the midst of the current crisis, federal agencies are now allowing mobile devices to access their enterprise networks out of pure necessity. However, when the crisis abates, many of these workers may advocate to continue working from home or at least using their own devices to access agency resources. Now's the time for agencies to start developing a telework solution strategy — not only to keep these teleworkers happy, but also to prepare the agency to respond more quickly in case future emergencies require a rapid shift to a 100% telework model.

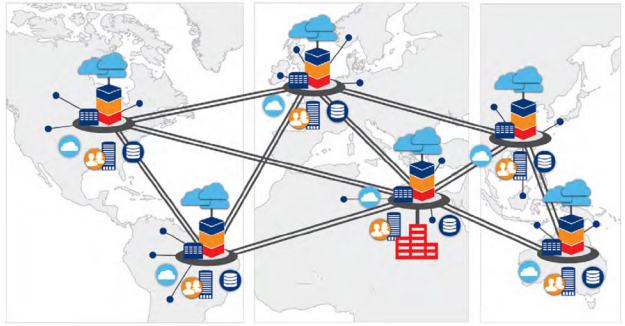
The reality is, we have been in the midst of a digital transformation for years, one that has been accelerated by the 2020 pandemic. It's forcing government agencies of all sizes to rapidly transition from legacy network approaches to mobility enabled by security controls in the cloud, on-premises, and on the modern endpoint.

Devices and the people using them have become the perimeter that an agency must monitor, manage, and secure. Is an authentication coming from a known endpoint? If so, is the user authorized to access the application? If not, does the posture of the device meet the security baseline and can we challenge the user for appropriate authentication?



Legacy Network Approach

- Internet service centrally controlled and expensive
- Single exit point for security control
- Poor network performance based upon location
- Company data on prem or in datacenter
- Network traffic backhauled to central location



Transformed Network Edge Approach

- Internet service distributed and commoditized
- Multiple points of entry / exit
- Regional service provides optimized network performance
- Direct connects to SaaS, IaaS, and globally distributed data centers
- Network traffic fast path out and moves to the edge (CDN)

In this BYOD era, organizations need a fully integrated security approach that covers the broadest set of OS and device offerings to effectively mitigate mobile threats while allowing the agility and anytime access that employees need. Traditional, static, perimeter-based, lock-down approaches to security don't cut it for the modern workplace. That's why many organizations are investing in and embracing zero trust security.

6 Ibid., https://csrc.nist.gov/publications/detail/sp/800-124/rev-2/draft

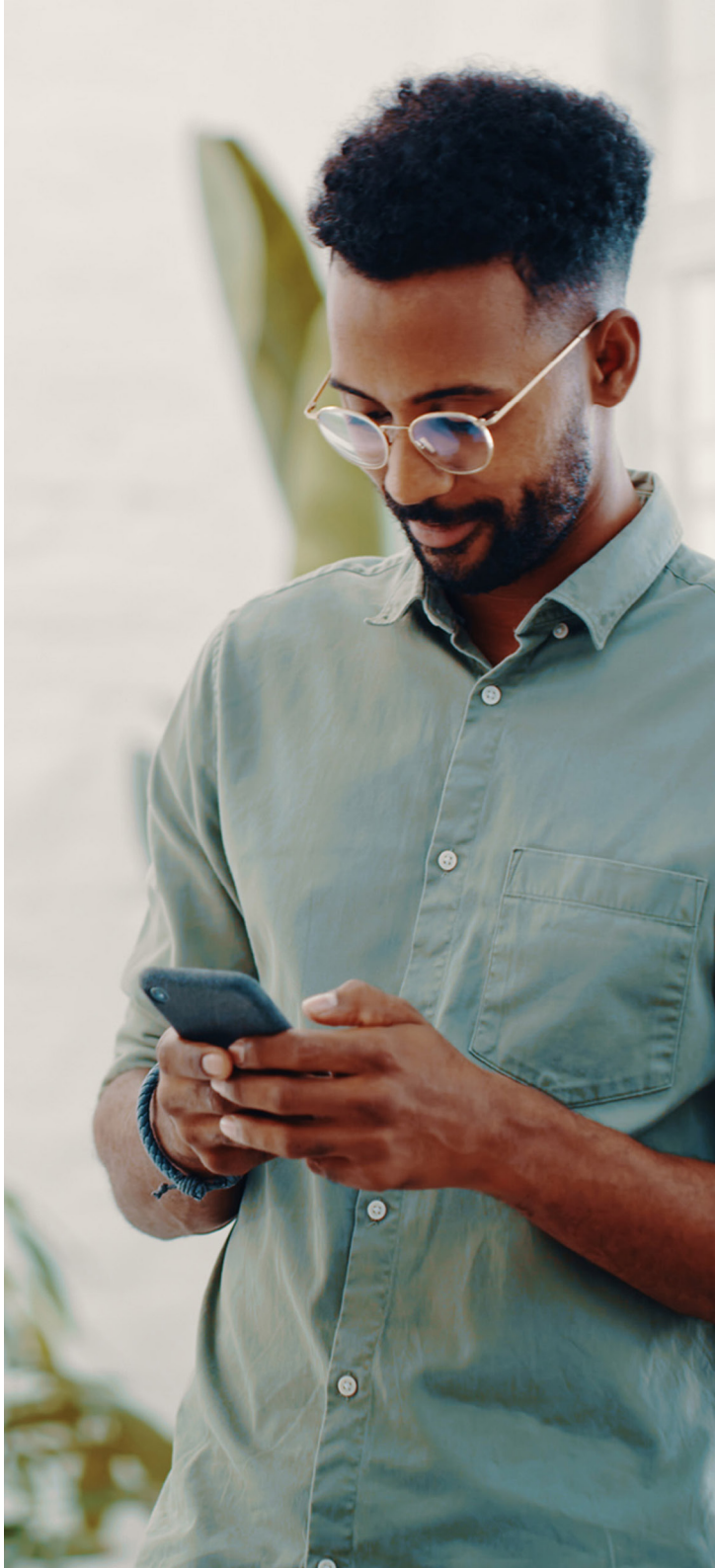
7 Graphic used by permission from OPAQ.com

FISMA Reporting and CDM

Federal agencies have begun to acknowledge and prepare for cybersecurity threats since at least 2005. Even then it was clear that these threats were present, often inside their hardened security perimeters. This awareness prompted discussions about insider vs. outsider threats and led the government to adopt a range of security controls that were codified in NIST SP 800-53. These controls became widely known as the Federal Information Security Modernization Act (FISMA) controls and led to significant improvements in cybersecurity.

FISMA requires agencies to implement and report on security controls based on NIST 800-53 control families. The reporting across federal agencies is normalized through the FISMA scorecards that agencies are required to prepare and the agency's CIO submits to the Department of Homeland Security (DHS). The DHS CDM dashboard provides enhanced information sharing, performance, visualization, and data analytics to both DHS and the agency itself. A lack of consistent measurement and the increasing risk of cybersecurity attacks, in part, resulted in developing standard requirements for agencies to provide cybersecurity threat diagnostics to DHS. The broad range of solutions used by federal agencies made synthesizing and analyzing the reporting data nearly impossible. Agencies lacked the budget, technical expertise, and guidance to develop common solutions that would enable real-time threat monitoring and information sharing among agencies.

Mobile devices are now included in the overall CDM program and are reported as part of the agency's FISMA scorecard. The inclusion of mobile device security controls follows that of traditional compute platforms. DHS has the mission to provide shared visibility across cybersecurity enforcement and emerging threats on endpoints used in federal agencies. This also requires reporting by the CIOs. The CDM also includes a solution to collect, analyze, report, and upload unified mobility security controls and risks to the government-wide cyber dashboard (EINSTEIN). By centralizing this data and reporting, EINSTEIN makes it easier for agencies to understand, anticipate, and share mobile device risks and vulnerabilities across multiple agencies



FISMA Mobility Metrics

Similarly, the Fiscal Year (FY) 2020 Chief Information Officer (CIO) FISMA reporting requirements now contains a section on mobility metrics (section 1.3), in which the Office of Management and Budget (OMB) requires federal agencies to report on mobile endpoints. Specifically, the OMB requires reports on the following: Determine the number of supervised mobile devices (Apple enrollment, Samsung Knox enrollment, etc.).

Determine if the supervised mobile device state is sufficient for asserting that administrator approval is required for profile removal. If true, count the number of devices meeting the condition.

Determine if the sub-component has MDM/EMM policy for a maximum time period for devices to run without updating to an identified OS or security update version level. If true, can and does the agency deny access when that time period is exceeded through the MDM/EMM tool? If true, count the number of devices meeting the condition.

Count the number of devices where the agency enforces the capability to prevent the execution of unauthorized software (e.g. blacklist, whitelist, or cryptographic containerization) through the MDM or EMM.

Count the number of MDM/EMM managed devices that require derived credentials for mobile device transactions (e.g. authentication, secure email).

In conjunction with the FISMA Mobility Metrics Working Group, Ivanti has produced a playbook on how to comply with the above FISMA Mobility Metrics reporting requirements. This playbook has been validated by the FISMA Mobility Metrics Working Group and by agencies that are successfully using it for their reporting. The document is available to federal agencies that are active Ivanti customers or on the OMB Max website at https://portal.max.gov/portal/home.

Ivanti supports CDM capabilities

CDM was originally defined with four phases, now referred to as capabilities, and summarized as “what is on your network” (asset management); “who is on your network” (identity and access management); “what is happening on the network” (network security management); and “how is data protected on your network” (data protection management). Ivanti enhances the agency’s discovery, controls and support for each of these capabilities.

“What is on the Network?” and “Who is on the Network?”

Before permitting a mobile device to access an agency’s enterprise network, Ivanti UEM acts as a policy decision point (PDP) that validates numerous contextual attributes to determine the risk of granting access to the applications or services requested. Ivanti UEM consists of two components — one that runs on the device (Android,iOS, MacOS, or Windows 10) and one that runs as a network server component either on-premises or in the cloud. Together, the components ensure compliance with the agency’s policies for security, user authentication, device compliance, and risk/threat detection and remediation.

Ivanti UEM registers the user’s device, pushes security policies, configurations, and an agency-managed profile to the user’s device, and tracks and manages the device’s OS, network, app versions, security patch compliance, encryption status, and geo-location. Ivanti then validates the user’s identity (on device authentication), the device’s identity, and the user’s credentials (including PIV/CAC derived credentials) and binds those attributes together as a part of the strong Identity, Credential, and Access Management (ICAM) policy compliance requirement. Ivanti also ensures that the mobile device is in compliance with all of the agency’s policy requirements before allowing the device to connect to the agency’s network. This allows the agency to whitelist and blacklist applications and networks, and provide dynamic contextual access control based on attributes from the device, network, user’s context, and environment.

If the device is out of compliance with any of the agency’s requirements, the Ivanti device-side component can function as a PEP, even when it’s not connected to any network or if it’s in “airplane mode.” The Ivanti Threat Defense (MTD) solution evaluates the threat posture of the device by detecting malicious code, phishing attempts, “man in the middle (MITM)” attacks, and other threats. MTD can then mitigate any threats on the device before allowing the device to connect to the enterprise network. If the device is out of compliance for any reason, Ivanti UEM can mitigate the risk through a continuum of actions. These can include blocking access to enterprise applications and data on the device, blocking access to the agency network and VPN, disabling Wi-Fi, or wiping the managed applications and data. Once the device is back in compliance, these actions can be reversed and the applications and data will be restored.

Ivanti also helps agencies address who is on the network by leveraging a secure gateway. This gateway uses the above contextual attributes along with strong multi-factor authentication to provide conditional access controls to enterprise applications and data as well as to cloud-based applications. This is critical because traffic to those cloudbased apps goes directly from the device to the cloud and typically does not transit the enterprise network. Therefore, any perimeter security controls are bypassed entirely, which can put agency data at risk. The secure gateway also ensures strong authentication by leveraging PIV/CAC derived credentials, other certificate-based authentication, or identity federation standards including SAML and FIDO2.

“What is Happening on the Network” and “How is Data Protected”

Awareness of what is happening on the network has always been a significant challenge, especially in complex infrastructures that include cloud, on-premises, and hybrid architectures. Protecting data on these complex networks requires a combination of monitoring, reporting, data leakage protections, and encryption. Ivanti can enforce data encryption in-transit, at rest, and in use.

Ivanti has joined forces with Splunk, Tenable, and other monitoring and reporting solutions to help agencies achieve greater visibility into their mobile data and the overall impact to the enterprise. With powerful monitoring and analytical insights, IT can intercept security threats, meet compliance requirements, and maintain the overall health of their information systems. This addresses a significant security gap many agencies face and that is frequently an issue in meeting compliance standards. Mobile device data and monitoring is typically only available in the silo of the EMM infrastructure and inaccessible to conventional security solutions. Ivanti has developed integrations and feeds to solve this, so that monitoring and sharing that data is easier, faster, and more productive across the enterprise.

Data leakage and exfiltration of agency data stored on or accessed by the mobile device is another significant threat that is only slowly being recognized by federal agencies. Many mobile devices have their own “native” productivity applications, such as email, bundled with them. When those applications aren’t managed by the agency, users may still be able to cut,copy, and paste from government applications into those native applications — a serious data breach. Ivanti enables IT to prevent copy/paste from managed apps and data into unmanaged areas of the device. Even for data that is controlled and managed, appropriate data protections require that the data be encrypted at rest, in use, and in motion. Ivanti UEM provides data encryption using the device’s native encryption as well as the Ivanti FIPS 140-2 compliant algorithms.

Conclusion

The DHS CDM program has matured and now includes mobile devices. Federal policies for BYOD and mobile devices in classified environments have been released in DoD. Agency requirements for meeting their mission critical demands all while staying in compliance requires trusted partners that can support agency needs today and into the future. Ivanti is that trusted partner. Our UEM platform can help federal agencies address CDM requirements, FISMA Mobility Metrics reporting, and other emerging mobile security requirements in an era of widespread teleworking.

About Ivanti

Ivanti makes the Everywhere Workplace possible. In the Everywhere Workplace, Federal employees and contractors use myriad devices to access IT networks, applications and data to stay productive as they work from anywhere. The Ivanti automation platform provides agencies industry-leading unified endpoint management, zero trust security and enterprise service management solutions, providing a single pane of glass for enterprises to self-heal and self-secure devices, and self-service end users. Many Federal Agencies and the Department of Defense as well as 78 of the Fortune 100, have chosen Ivanti to discover, manage, secure and service their IT assets from cloud to edge to enterprisee, and deliver excellent end user experiences for workers, wherever and however they work. For more information,visit ivanti.com

ivanti.com
1 800 982 2130
sales@ivanti.com