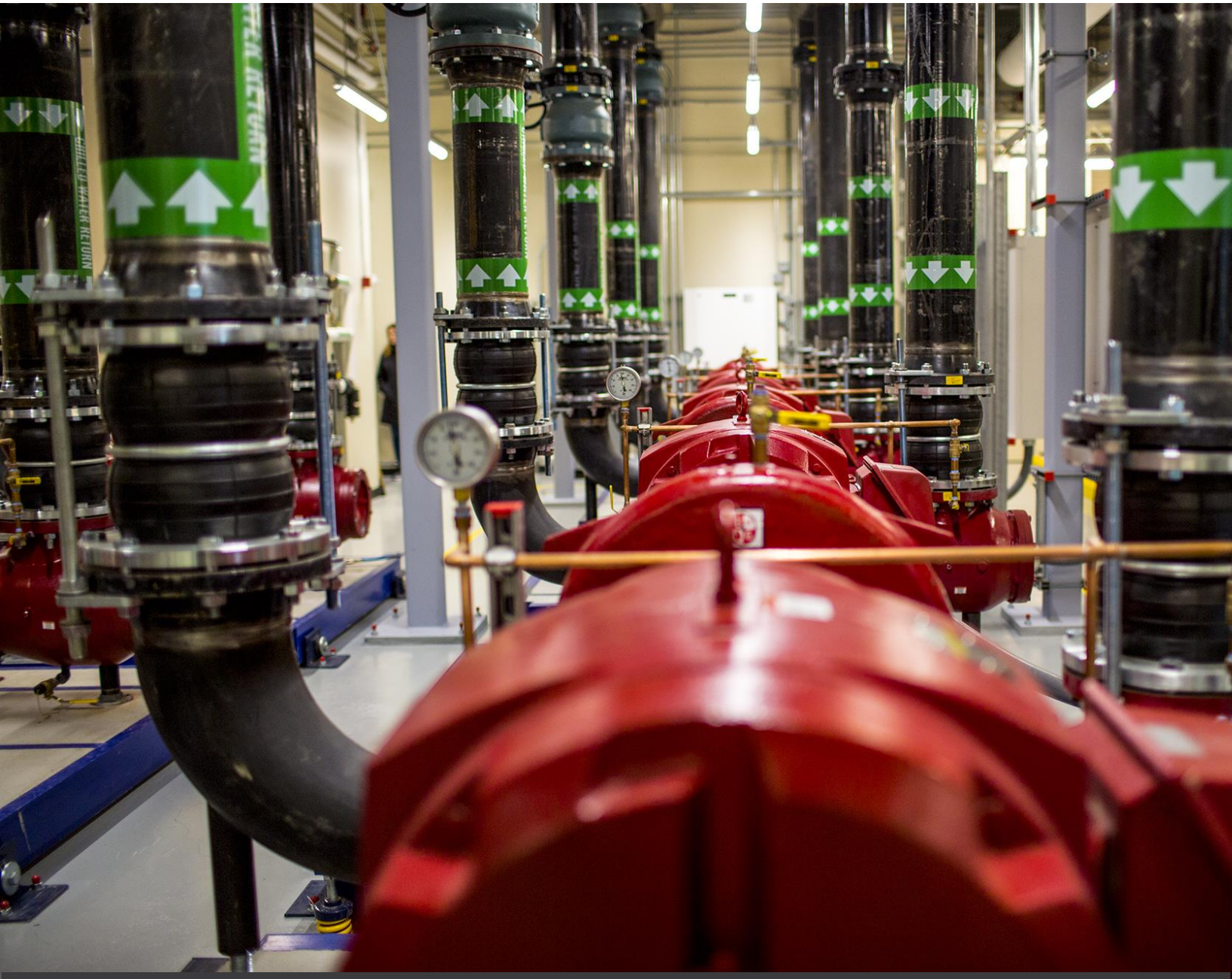


Microsoft

Department of Energy

Request for Information – Ensuring the Continued Security of the United States Critical Electric Infrastructure

Solicitation Number: 6450-01-P

June 07, 2021

Submitted to:

Michael Coe
Director, Energy Resilience Division of the Office of Electricity
U.S. Department of Energy, Mailstop OE-20, Room 8H-033, 1000 Independence Avenue, SW, Washington, DC 20585
(202) 287-5166
ElectricSystemEO@hq.doe.gov

Table of Contents

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

The descriptions of other companies' products in this document, if any, are provided only as a convenience to you. Any such references should not be considered an endorsement or support by Microsoft. Microsoft cannot guarantee their accuracy, and the products may change over time. Also, the descriptions are intended as brief highlights to aid understanding, rather than as thorough coverage. For authoritative descriptions of these products, please consult their respective manufacturers.

June 07, 2021

Lori Knerr
One Microsoft Way
Redmond, WA 98052

Dear Mr. Coe,

Enclosed with this letter please find Microsoft's response to the Office of Electricity, Department of Energy Request for Information to ensure the continued security of the United States critical electric infrastructure. We realize the magnitude and importance of this inquiry; our response demonstrates the depth of how we can partner with you to continue to ensure the resiliency of our Nation's critical infrastructure in a more digital world. Securing critical infrastructure is not an easy task. Nation-state actors deploy sophisticated cybercampaigns to disrupt daily life or spread confusion. The power grid is one such target. All modern infrastructure including our defense, transportation, communication, hospitals, and financial institutions require secure, reliable access to energy and the internet to function.

Implemented Internet of Things (IoT) innovations allow the utility industry to harness the power of the internet, data, and artificial intelligence (AI) to optimize its operations and deliver energy more efficiently and reliably to its customers, but these devices can introduce new vulnerabilities. Existing sensors often don't have security or centralized management built into them. Some devices are so small, it's difficult to place traditional protections on them. Manufacturers, who feel pressured to deliver solutions quickly, may fail to incorporate critical security controls and safeguards in their products. Bad actors are skilled at uncovering these weaknesses and exploiting them. New technologies, especially in distributed generation and storage, continue to hit the market along with existing technologies for distribution and transmission, further increasing potential vulnerability. Security architecture must accommodate traditional closed systems such as the traditional production, transmission, and distribution method as well as emerging edge systems such as electric vehicle charging stations, private microgrids, and residential renewable energy systems.

As modern infrastructure becomes more reliant on connected devices, the power industry must continue to come together to improve security at every step of the process. We recognized that it would take more than just one entity to create a more secure infrastructure here in the United States and are collaborative partners with the Department of Energy and its vendors to help improve cyber supply chain risk management, adopt a Zero Trust secure model for the electric infrastructure, and develop a long-term strategy that will adopt a continuous evolving digital environment. Microsoft has shared our perspective relative to preventing exploitation and attacks by foreign threats to the United States supply chain from a secure framework approach in compliance with widely adopted federal and commercial standards. Our recommendations include ways to improve cyber supply chain risk management, implementing a Zero Trust security model, defending against supply chain attacks, protecting against malware, and employing a comprehensive monitoring program as part of the Departments long term strategic development.

Lori Knerr
Account Strategy Executive Innovation and Science
Microsoft – United States Department of Energy
Phone: 301-771-8744
lknerr@microsoft.com

1 Request for Information Comments

The Department of Energy (DOE) has a pressing responsibility to ensure the continued security of the United States Critical Electric Infrastructure. Microsoft has provided a response to this request for information from a technical capability perspective in line with industry's current practices to identify and mitigate perceived supply chain vulnerabilities. We understand the DOE enterprise scale and areas of opportunities to improve its security, along with the quality, timeliness, and cost of services. The following sections represents key considerations when developing a long-term security strategy.

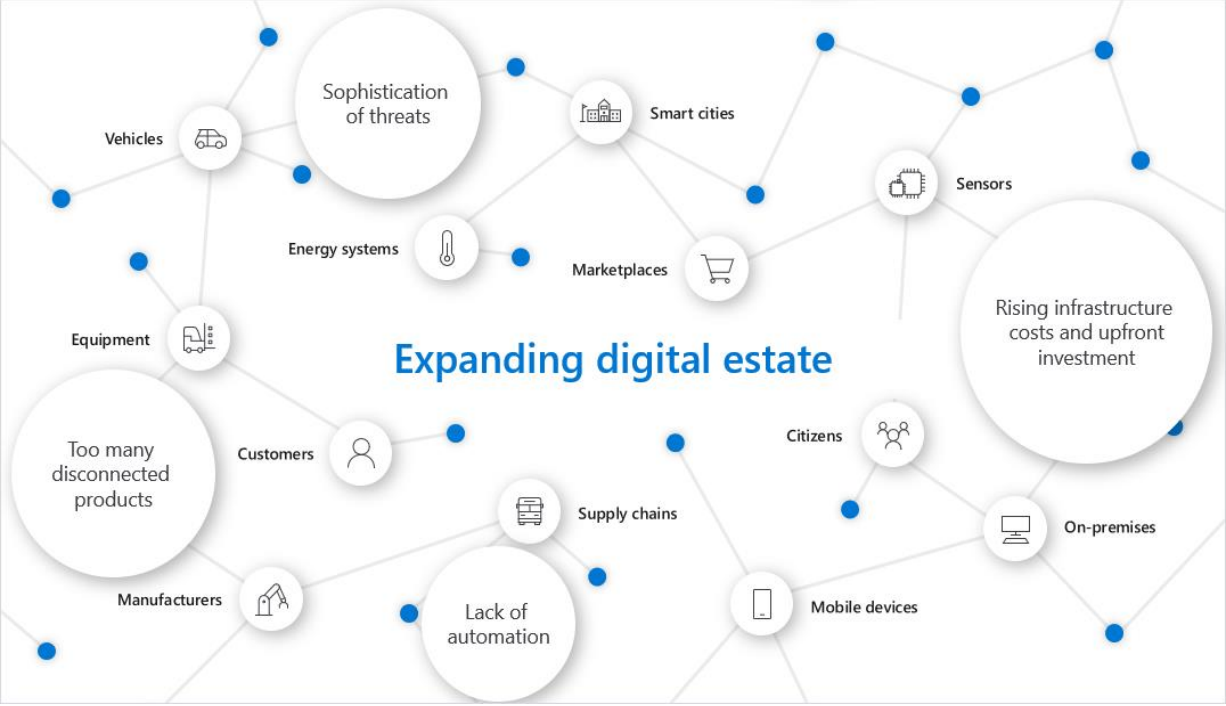
1.1 Improve Cyber Supply Chain Risk Management

An unsecured supply chain can introduce great risk to an organization. If vendor staff aren't properly vetted or if hardware is purchased that does not meet security standards, an organization can lose data. On industry average, it is estimated it takes 229 days after a breach for it to be detected. Often, these breaches are found to be caused by a vulnerability in third-party software or services being exploited, costing those companies tens of millions of dollars and damaging customers' confidence.

An organization is only as strong as its weakest link. The factories that build Microsoft products must have a secure infrastructure to ensure that manufacturing data and facilities are secure. Some of the benefits we have seen from introducing a security framework as part of the procurement process include:

- **Reduced risk**. Supply chain security services help us proactively address compliance or security issues and reduce financial and legal exposure.
- **Operational efficiencies**. Standardized governance and lifecycle management processes have helped streamline our fulfillment processes.
- **Cost savings**. Our strategic alignment with competitive technology objectives helps us avoid unnecessary software purchases.
- **Risk-informed decision making.** We assess procurement requests and make recommendations to business groups and leadership teams that help them make more risk-informed decisions.

For years, Microsoft has tracked threat actors exploiting federal cyber supply chain vulnerabilities. Supply chain attacks target software developers, systems integrators, and technology companies. Tactics often include obtaining source code, build processes, or update mechanisms to compromise legitimate applications. This is a key concern for government cybersecurity in the cloud, as the expanding digital estate requires movement towards a Zero Trust security model illustrated below.



At Microsoft, supply chain security means holding our suppliers to the same security standards we apply to ourselves. This is mission critical for our customers and for Microsoft as we own and operate one of the largest backbone networks in the world; spanning more than 165,000 miles and 61 Azure regions strategically placed around the world. To deliver optimal supply chain assurance globally, Microsoft created a program that helps us assess security in third-party software, goods, and services during procurement; and we would be more than happy to collaborate with DOE to do the same. Our framework consists of a supplier risk profile and assessments that produce risk indicators and recommend actions. Assessing suppliers helps to reduce risk in the supply chain and make risk-based decisions.

Whether it's caused by poor quality control, or a malicious actor, third-party software, solutions, and manufacturers can introduce risk to corporate, employee, and customer data. Microsoft is committed to building and implementing best-in-class security programs and processes and is constantly working to reduce exposure to cybersecurity risks. Microsoft Core Services Engineering (CSE), formerly Microsoft IT, helps support the overall security mission at Microsoft by offering key security services that help protect corporate data and users. We are also securing the supply chain that we use to procure third-party software, goods, and services that are used at Microsoft.

1.2 Zero Trust to Secure our Electric Infrastructure

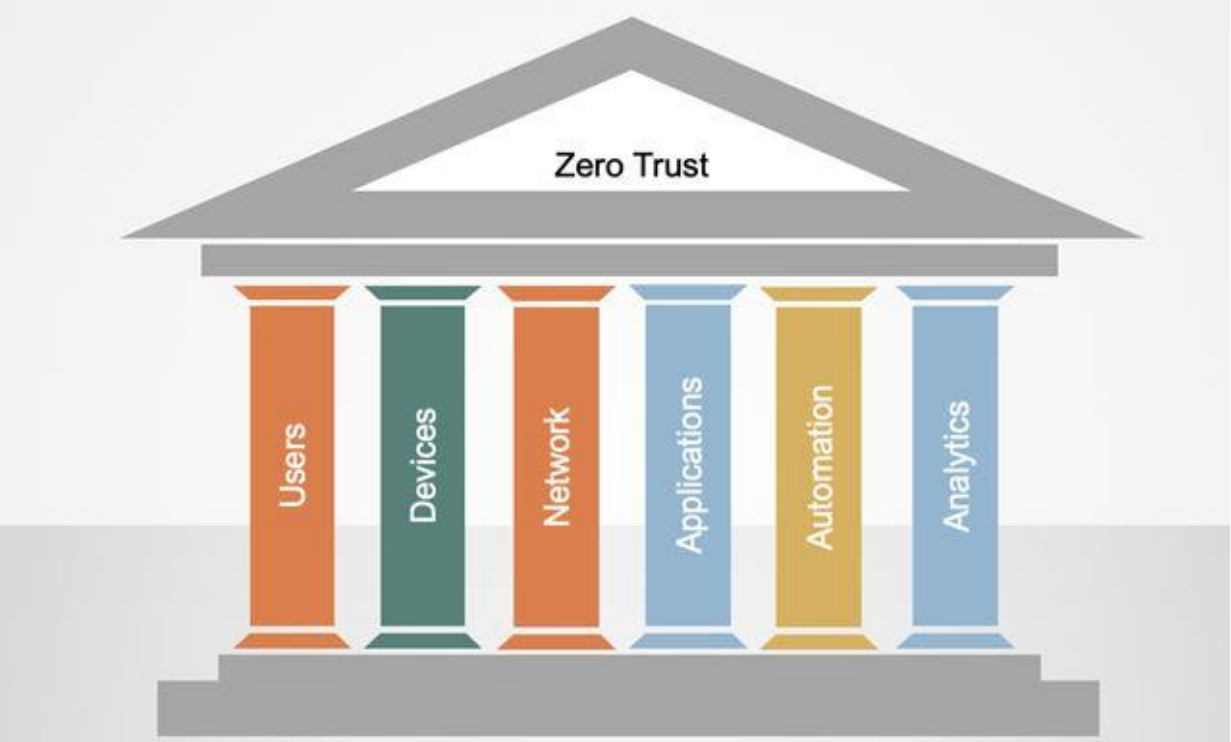
Microsoft outlines three principles of Zero Trust - Verify Explicitly, Least Privilege Access and Assume Breach. Assume breach is a mindset we must take beyond the enterprise to consider our partners, contractors, and suppliers. National Institute of Standards and Technology (NIST) SP 800-207 for Zero Trust Architectures recommends organizations "should evaluate service providers on a holistic basis by taking into consideration factors such as vendor security controls, enterprise switching costs, and supply chain risk management."[i] Supply Chain Risk

Management is the process of securing vendors, partners and supply chains to prevent disruption to the organization. Threat actors target these assets to gain a foothold in a network and attacks can include:

- Compromise of software building tools to ensure malware is imprinted into all software generated from the building tools.
- Replacing software update repositories with malicious replicas that distribute malware across entire software ecosystems.
- Steal code-signing certificates to make malicious software appear as legitimate code.
- Intercept hardware shipments to inject malicious code into hardware, firmware, and field-programmable gate arrays (FPGAs).
- Pre-install malware onto IoT devices before they arrive to target organizations.

As a result, Microsoft Azure has developed a nine-step process to facilitate supply chain risk management for federal information systems in Microsoft Azure which is aligned with the security monitoring principles within the TIC 3.0, NIST CSF and NIST SP 800-161 standards. Note this process is a starting point, as supply chain risk management programs require alignment of people, processes, policy, and technology to be optimally successful.

Zero Trust can be thought of as a strategic initiative that, together with an organizing framework, enables decision makers and security leaders to achieve pragmatic and effective security implementations. Zero Trust efforts need to incorporate, coordinate, and integrate a challenging combination of policies, practices, and technologies to succeed. A conceptual security model can be helpful to understand and organize those components. The figure below illustrates the six Pillars of a Zero Trust security model.



Pillar #1 – User - People/Identity Security. Ongoing authentication of trusted users is paramount to Zero Trust. This encompasses the use of technologies like Identity, Credential, and Access Management (ICAM) and multi-factor authentication and continuously monitoring and validating user trustworthiness to govern their access and privileges. Technologies for securing and protecting users' interactions, such as traditional web gateway solutions, are also important.

Pillar #2 – Devices - Device Security. Real-time cybersecurity posture and trustworthiness of devices is a foundational attribute of a Zero Trust approach. Some "system of record" solutions such as asset management solutions provide data that can be useful for device-trust assessments. In addition, other assessments should be conducted for every access request (e.g., examinations of compromise state, software versions, protection status, encryption enablement, etc.).

Pillar #3 – Network - Network Security. Zero Trust Networks are sometimes described as "perimeterless", however this is a bit of a misnomer. Zero Trust Networks attempt to move perimeters in from the network edge and segment and isolate critical data from other data. The perimeter is still a reality, albeit in much more granular ways. The traditional infrastructure firewall perimeter "castle and moat" approach is not sufficient. The perimeter must move closer to the data in concert with micro-segmentation to strengthen protections and controls. Network security is expanding as agencies grow their networks to transition to Software Defined Networks, Software Defined Wide Area Networks, and internet-based technologies partially or fully. It is critical to (a) control privileged network access, (b) manage internal and external data flows, (c) prevent lateral movement in the network, and (d) have visibility to make dynamic policy and trust decisions on network and data traffic. The ability to segment, isolate, and control the network continues to be a pivotal point of security and essential for a Zero Trust Network.

Pillar #4 – Applications - Application and Workload Security. Securing and properly managing the application layer as well as compute containers and virtual machines is central to Zero Trust adoption. Having the ability to identify and control the technology stack facilitates more granular and accurate access decisions. Unsurprisingly, multi-factor authentication is an increasingly critical part of providing proper access control to applications in Zero Trust environments.

Pillar #5 – Automation - Security Automation and Orchestration. Zero Trust makes full use of security automation response tools that automate tasks across products through workflows while allowing for end-user oversight and interaction. Security Operation Centers commonly make use of other automated tools for security information and event management and user and entity behavior analysis. Security orchestration connects these security tools and assists in managing disparate security systems. Working in an integrated manner, these tools can greatly reduce manual effort and event reaction times and reduce costs.

Pillar #6 – Analytics - Security Visibility and Analytics. Zero Trust leverages tools like security information management, advanced security analytics platforms, security user behavior analytics, and other analytics systems to enable security experts to observe in real time what is happening and orient defenses more intelligently. The focus on the analysis of cyber-related event data can help develop proactive security measures before an actual incident occurs. Holistically, the six pillars of Zero Trust provide risk reduction and mitigation for Information Technology (IT) and Operational Technology (OT) networks along with supply chain threat vectors.

There are several techniques to attack cyber supply chains in Information Communications and Technology (ICT) products and services. Supply chain attacks are most concerning because they target vulnerabilities in your infrastructure before you even deploy your assets and software. Attackers can:

- Compromise software building tools to ensure that their malware is imprinted into all software generated from the building tools.
- Replace software update repositories with malicious replicas that distribute malware across entire software ecosystems.
- Steal code-signing certificates to make malicious software appear as legitimate code.
- Intercept hardware shipments to inject malicious code into hardware, firmware, and field-programmable gate arrays (FPGAs).
- Pre-install malware onto Internet of Things (IoT) devices before they arrive to target organizations.

1.3 Managing Supply Chain Risk Management to Defend Against Supply Chain Attacks

Defending against supply chain attacks requires a comprehensive approach to managing Supply Chain Risk Management (SCRM). Federal risk managers must deploy strong code integrity policies and technical screening controls to ensure their software complies with organizational directives such as applying NIST SP 800-53A security controls for Federal Information Security Management Act (FISMA) compliance. Code integrity requires full non-repudiation of software to validate information producer associations, identity, and chain of custody for systems and components (NIST SP 800-161, 2015). One critical opportunity for addressing code integrity in your supply chain is to implement and adhere to a secure software development lifecycle for applications that you develop in-house and that you acquire from third-party supply chain partners.

Microsoft continues to use the Security Development Lifecycle, a fundamental process of continuous learning and improvement in the security, integrity, and resiliency of our enterprise applications. We require supply chain providers to adhere to these practices as well.

Organizations should employ asset monitoring and tracking systems such as radio-frequency identification (RFID) and digital signatures to track hardware and software from producers to consumers to ensure system and component integrity. Federal Information Processing Standards (FIPS) 200 specifies that federal organizations “must identify, report, and correct information and information system flaws in a timely manner while providing protection from malicious code at appropriate locations within organizational information systems” (FIPS 200, 2006).

Reference: Securing the supply chain with risk-based assessments (microsoft.com)

1.4 Protecting Against Supply Chain Attacks – Malware

Supply chain attacks are an emerging kind of threat that target software developers and suppliers. The goal is to access source codes, build processes, or update mechanisms by infecting legitimate applications to distribute malware. Attackers hunt for unsecure network protocols, unprotected server infrastructures, and unsafe coding practices. They break in, change source codes, and hide malware in build and update processes.

Endpoint Protection Platforms can support software development and fight malware, but government organizations must follow recommendations for software vendors and developers by applying patches for operating systems and software, implementing mandatory integrity controls, and requiring Multi-Factor Authentication (MFA) for administrators.

Security of federal information systems requires compliance with stringent standards such as NIST SP 800-53, FISMA, Center for Internet Security (CIS) Benchmarks, and FedRAMP Moderate. Maintaining compliance with these standards ensures a secure-by-design approach to federal information security. Defining a repeatable set of resources that implement and adhere to an organization's standards, patterns, and requirements helps maintain a highly secure build and updated infrastructure. Implementing role assignments, policy assignments, and Resource Manager templates helps build secure software updates as part of the Software Development Lifecycle and provides a framework to directly apply compliance requirements to your environment while monitoring configurations through Continuous Monitoring (CM).

Microsoft provides multi-layer IoT security in Azure, which is being used by thousands of customers in production and has made securely configuring IoT devices possible.

1.5 Employing a Comprehensive Monitoring Program

Protecting your supply chain requires a comprehensive monitoring program with cyber incident response and security operations capabilities. Built-in artificial intelligence (AI) helps analyze large volumes of data across an enterprise. Data aggregation from all sources, including users, applications, servers, and devices running on-premises or in any cloud lets you reason over millions of records in a few seconds.

Analytics allow cyber defenders to employ proactive alerting to detect threats impacting your supply chain security. This capability allows federal agencies to compensate for the cyber talent gap with Security Automation & Orchestration Response (SOAR) capabilities while leveraging machine learning and AI capabilities.

DOE should consider hunting search-and-query tools that are based in the MITRE ATT&CK Framework, allowing your responders to proactively hunt threats across the network before alerts are triggered.

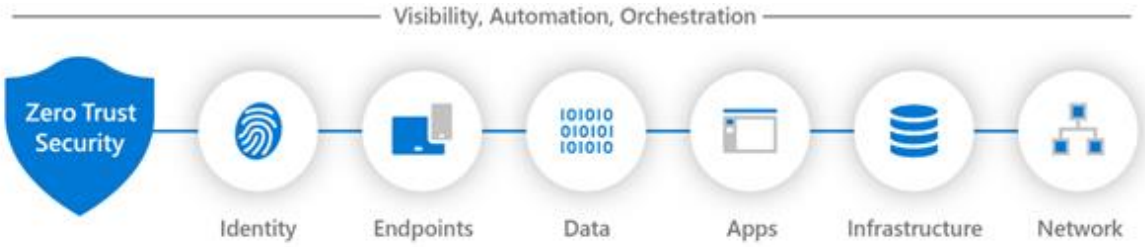
SCRM is a growing focus within the federal sector. Microsoft is committed to bolstering government cybersecurity in the cloud.

2 A. Development of a Long-Term Strategy

1. What technical assistance would States, Indian Tribes, or units of local government need to enhance their security efforts relative to the electric system?

A Zero Trust Architecture is central to enhancing security of the electric system. The Zero Trust model teaches us to "never trust, always verify." the three guiding principles of Zero trust are:

1. **Verify explicitly**. Always authenticate and authorize based on all available data points.
2. **Use least privileged access**. Limit user access with Just-In-Time and Just-Enough-Access (JIT/JEA), risk-based adaptive policies, and data protection.
3. **Assume breach**. Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses.



An integrated set of solutions and capabilities offer built-in Zero Trust controls that make implementing a Zero Trust security model across your organization achievable at scale. We have industry solutions for identity and access management, endpoints, data and applications, infrastructure and network described below.

Identity and Access Management (IDAM). Azure Active Directory provides greater control over identity threats. Capabilities like Role based access control (RBAC), multi-factor authentication (MFA), and identity protection will help ensure the right users are getting the appropriate level of access. The hybrid world is largely perimeterless, so wrapping protections around identity and devices is critical. Azure AD integrates with passwordless technologies such as Microsoft Authenticator, Windows Hello, FIDO2 security keys, and biometrics. Azure AD can be easily synchronized with on-premises Active Directory, connected to cloud HR systems, and enabled for external users. Enable Single Sign On with Azure AD to all apps including Software-as-a Service (SaaS) apps, custom built cloud apps, and on-prem apps. Azure AD Application Proxy is a feature of Azure AD that enables users to access on-premises web applications from a remote client. Microsoft Defender for Identity protects on-premises identities with cloud power and intelligence at each stage of the attack life cycle and identity hygiene is reflected in Microsoft Secure Score.

Endpoints. Microsoft Defender for Endpoint is a holistic, cloud-delivered endpoint security solution. Its capabilities include risk-based vulnerability management and assessment, attack surface reduction, behavior-based next-generation protection, Endpoint Detection and Response (EDR), automatic investigation and remediation, managed hunting services, rich APIs, and unified security management. Microsoft Endpoint Manager includes the services and tools you

use to manage and monitor mobile devices, desktop computers, virtual machines, embedded devices, and servers. Endpoint Manager combines services you may know and already be using, including Microsoft Intune, Configuration Manager, Desktop Analytics, co-management, and Windows Autopilot.

Microsoft Azure offers several IoT services that provide Zero Trust capabilities, such as Azure IoT Hub, Azure IoT Hub Device Provisioning Service (DPS), Azure Device Update for IoT Hub, and Azure Defender for IoT. Microsoft offers edge platforms including runtimes such as Azure IoT Edge and Azure IoT platform SDKS, and operating systems including Azure Real Time Operating System (RTOS) and Windows 10 IoT Enterprise. Microsoft also offers lightweight endpoint security agents that interoperate with Azure IoT Hub and Azure Defender for IoT, with support for both Microsoft and Linux IoT platforms. For device builders to reflect that their device offers Zero Trust capabilities, they should get the Edge Secured-core certification, one of the certifications in the Azure Certified Device program. Microsoft also offers Zero Trust devices ready to meet your needs, including Azure Sphere and Azure Percept.

Data. Ultimately, security teams are focused on protecting data, protect your sensitive data wherever it lives or travels. Data encryption controls are built-in to Microsoft services from virtual machines to storage, SQL, CosmosDB and Azure Data Lake. Azure Key Vault enables you to safeguard and control cryptographic keys and other secrets used by cloud apps and services. Microsoft Information Protection (MIP) provides a unified and consistent approach to inspecting and classifying data across locations and repositories. Azure Information Protection (AIP) is part of the MIP solution, and extends the labeling and classification functionality to the cloud.

Applications. Applications and APIs provide the interface by which data is consumed, they may be legacy on premises, lift and shifted to cloud workloads, or modern SaaS applications. Implement real-time protection against cyberthreats, anomalies, and grant appropriate access for every app based on the user and the device they are on from any network location. Microsoft Cloud App Security is our Cloud Access Security Broker (CASB) solution. Microsoft Cloud App Security uses user and entity behavioral analytics (UEBA) and machine learning (ML) to detect unusual behavior across cloud apps, enabling us to identify ransomware, compromised users or rogue applications, analyze high-risk usage, and remediate automatically to limit the risk to your organization.

Infrastructure. Infrastructure (whether on premises servers, cloud based VMs, boxes, or micro services) represents a critical threat vector. Azure Security Center continuously assesses the security state of your cloud resources across virtual machines, networks, applications, and data services. It even monitors server workloads running in other clouds and on-premises datacenters. Its cross-cloud capabilities help you visualize your security state and quickly get insights on your configured security controls. Azure Secure Score is the core of Azure Security Center's security posture management capabilities.

Network. All data is ultimately accessed over network infrastructure. Networking controls can provide critical "in pipe" controls to enhance visibility and help prevent attackers from moving laterally across the network. Networks should be segmented (including deeper in network micro segmentation) and real time threat protection, end to end encryption, monitoring, and analytics should be employed. For network security you can establish secure connections to and within Azure using virtual networks, network security groups, VPN, and ExpressRoute. Protect and

ensure availability of your apps, protect against network layer threats with services like Web Application Firewall, Azure Firewall and Azure denial of service.

Threat Protection & Security Management. It is equally important to continuously monitor the state of security, especially as cloud workloads change dynamically. Microsoft Defender integrates Security Information and Event Management (SIEM) and Extended Detection and Response (XDR) tools providing end-to-end threat visibility across all your resources. Microsoft Defender is delivered in two tailored experiences, Microsoft 365 Defender for end-user environments and Azure Defender accessed within Azure Security Center. Azure Security Center will help you monitor the security state of Azure resources and hybrid workloads, providing a dynamic security score card.

Azure Sentinel is our cloud native SIEM and SOAR technology. Sentinel makes it easy to collect security data across your entire hybrid organization from devices, users, apps, servers, and any cloud, it uses the power of artificial intelligence to ensure you are identifying real threats quickly. Sentinel can automatically detect multistage attacks by identifying combinations of anomalous behaviors and suspicious activities that are observed at various stages of the kill-chain and uses the MITRE ATT&CK framework to establish a common industry nomenclature. Use Azure Lighthouse and Azure Sentinel to Investigate Attacks Across Multiple Tenants. We recommend using a distributed deployment and centralized management model. This is where you deploy Azure Sentinel workspaces within the tenant that belongs to the customer or subsidiary (data stays locally within the customer's or individual subsidiary's environment) and manage it centrally from within a service provider's or from a central security operations center (SOC) unit's tenant within an organization.

2. What specific additional actions could be taken by regulators to address the security of critical electric infrastructure and the incorporation of criteria for evaluating foreign ownership, control, and influence into supply chain risk management, and how can the Department of Energy best inform those actions?

The DOE plays an important role in mitigating supply chain risks across the electricity sector by increasing education and awareness of threats and by setting forth heightened standards and best practices. The first step is to assist operators in identifying risks and threats to the security and resiliency of their supply chains.

At Microsoft, in the context of malicious threats, we think it's important to consider the risks of:

- **Manipulation** – The alteration of technology, data, or processes, enabling unintended control, unwanted functionality, or obscured understanding of functionality or results.
- **Espionage** – The observation of confidential information at any point in the new ecosystem of digitally and operationally converged technology.
- **Disruption** – From sabotage or full denial of service to degradation of reliability or trustworthiness.

The next steps in coordinating an architecture across the diverse technologies and services afforded by our third-party ecosystem require correlating these three risks to impacts. Those impacts are:

- **Tainted solutions** – Whether hardware, software or cloud-based services, the threats identified manifest in the potential for taint — a solution that no longer functions as its designer or user intended.
- **Counterfeit solutions** – Functional integrity and quality are compromised when deceptively "real" looking and functioning technology is put into operation.
- **Intellectual property misuse** – The lifeblood of innovation, intellectual property (IP), when disclosed in whole or in part, can be effectively leveraged to manipulate, falsify, and create tainted and counterfeit solutions.
- **Outage** - Lapses in processes, people, redundancy, resilience, failure of a key dependency or a lack of confidence cause a product or service to be unusable preventing the continuity of operation.

We urge the Department to clearly articulate threats to the security or resiliency of the supply chain and help operators assess specific risks to their own operations. An approach that focuses on flexibility (as opposed to more prescriptive mandates) will help operators remain agile during rapidly changing technology, security threats, and supply chain risks.

Leveraging Supply Chain Security Solutions. Microsoft understands firsthand that in an age of accelerating digital transformation and increasingly sophisticated threats, global supply chain security is more important, and more complex, than ever. Critical to achieving supply chain security today is the ability protect against transnational threats and ensure the resiliency of critical technology and supplies in a tumultuous environment. This requires cross-industry and cross-government alignment in efforts to strengthen software and hardware supply chains and IT infrastructure for all sectors, including vulnerable critical electric infrastructure.

Microsoft has promoted incentivizing digital solutions to mitigate supply chain risk, and recently submitted to the U.S. government alternative mechanisms to mitigate security threats and enhance the resiliency of the supply chain. Until now, governments and non-government actors have attempted to protect supply chains through piecemeal restrictions. A more comprehensive, targeted and technology-enabled strategy is needed. Key to this strategy is an approach that first clearly and carefully identifies key supply chain risks and then, creates incentives for the adoption of best practice mitigation strategies, including digital solutions that target these risks without restricting trade altogether. In recent submissions to the Department of Commerce (Regulations.gov (for Docket DOC 2019-0005), we offered several existing risk-mitigating technologies that can be more widely deployed to bolster supply chain security, including:

- **Software security technologies** designed into software packages or code can address security risks by ensuring trust and preventing software from being exploited by bad actors or for malignant uses. These features include: the ability to deploy trusted software updates, including the firmware of compromised devices; automating security policies to, for example, seek out and prevent placement of user or administrator credentials in software code; and, in appropriate cases once in-development standards are finalized, use of software bills of materials (SBOMs) to convey evidence that software consumers can trust the environment in which software was built.
- **Hardware security technologies** built into hardware can further protect against supply chain risks. Solutions include hardware roots-of-trust to verify, protect or restore system,

data, or code integrity; secure co-processors for more robust identity verification; and, in appropriate cases, origin and identity attestation for components in a hardware system.

- **Data security technologies** can protect exposure of U.S. data through the supply chain. Features include digital rights management, information flow controls, data tagging and, where appropriate, the use of secure virtual or data lockbox environments.

Future innovations in each of these areas, including more advanced security processors that tie hardware, code, and data more closely, and artificial-intelligence-based solutions, are also underway.

We urge the DOE to consider accelerating the development of these solutions by providing incentives for companies to adopt the best practices and technology-enabled solutions designed to mitigate key supply chain risks. In the long run, such incentives will expand the market for these tools, leading companies to allocate more resources to the development of more advanced and effective risk mitigation technologies.

Leveraging Digital Transformation and use of Cloud-based Solutions. The security of critical electric infrastructure can be greatly enhanced by incentivizing operators to adopt cloud-based solutions that incorporate advanced security services and offerings. The DOE should therefore look to incentivize digital transformation as it considers options to improve the overall security posture of the sector.

The DOE should consider how critical electric infrastructure are leveraging the Framework for Improving Critical Infrastructure Cybersecurity v1.1 (NIST Cybersecurity Framework) and NIST's supply chain risk management guidance. Furthermore, NIST is in the process of updating its Cyber Supply Chain Risk Management guidance (NIST 800-161) to better support supply chain security. DOE should consider any policy mechanisms it leverages to consider a close alignment with recent Cyber Executive Order (EO) requirements for federal agencies.

We encourage the DOE to consider any actions taken on security in collaboration and alignment with other agencies including Office of Management and Budget (OMB), the Federal Acquisition Security Council (FASC), NIST, and Department of Homeland Security (DHS) in addition to the National Cyber Director role and the Federal Chief Information Security Officer (CISO) role which can facilitate more robust cross-government coordination on similar issues and implementation of existing as well as in-development cyber and supply chain risk management best practices.

As a leading hyper-scale Cloud Service Provider (CSP), Microsoft offers comprehensive and secure cloud computing services, including servers, storage, databases, networking, software, analytics and more, that are available through a common cloud infrastructure and platform. Customers can choose to access cloud via a dedicated communication network that is offered by Microsoft, thereby eliminating the need to rely on an internet connection. Further, customers requiring increased security can access dedicated cloud platforms through direct communications networks, avoiding the need for internet facing ports. Accordingly, Azure is not just a remote storage resource – it is a set of services that are designed to assist users, including electric utilities, meet their business objectives while adhering to the most stringent regulatory and security standards. Most cloud computing services are provided as self-service and on demand, so that even vast amounts of computing resources can be setup in minutes, typically with just a few mouse clicks, giving businesses a great deal of flexibility without having to make continuous and potentially significant capital investments.

Azure's cloud-based offerings and its security have evolved significantly since their inception, and this evolution has continued following the Commission's issuance of the Notice of Inquiry (NOI) in this proceeding, far surpassing the capabilities that electric utilities might be able to provide on-site. Microsoft annually invests over $1 billion in cybersecurity, which far exceeds the cybersecurity investments of any Registered Entity. Accordingly, Azure offers advantages for any sized utility to deploy its critical workloads, but Azure would be especially useful for smaller utilities that lack budget for large compliance and security teams.

3. What actions can the Department take to facilitate responsible and effective procurement practices by the private sector? What are the potential costs and benefits of those actions?

For both software and hardware security, any procurement requirements should leverage existing best practices for the entire product lifecycle. DOE will achieve an integrated security philosophy and end-to-end strategy by implementing Zero Trust controls and technologies across six foundational elements: identities, devices, applications, data, infrastructure, and networks. Each of these six foundational elements is a source of signal, a control plane for enforcement, and a critical resource to be defended. This makes each an important area to focus investments. Model procurement requirements should integrate existing best practices for secure development, as captured by the Security Development Lifecycle and International Organization for Standardization (ISO) 27034, including:

- Threat modeling, software sourcing (i.e., managing risks of third-party components), and security testing.
- Vulnerability management, including through coordinated vulnerability disclosure.
- Use of integrity controls throughout the software development, testing, and delivery processes.
- Publication of a lifecycle policy, committing to a support period during which security issues will be addressed.

To facilitate responsible and effective procurement practices, Microsoft believes that the Nation's energy and national security will be best served through a three-pronged effort by the government to utilize digital technology. First, the government should use commercially available technology when it is sufficient for the task and as the foundation for additional development when more work is needed. This will both accelerate speed and reduce costs. Second, the government should add security layers to commercial technology when required, such as by protecting highly sensitive critical infrastructure workloads. Third, the government should adapt commercial products and development methods for energy sector uses and applications, including through additional product development that breaks down barriers between engineers in the private sector and critical infrastructure providers and those in the public sector.

This could also include incentivizing information sharing of threat intelligence across the critical electric infrastructure sector, including a clear, consistent disclosure obligation on the private sector. Timely threat intelligence can help defend against cyberattacks today. But only if threat intelligence is shared quickly and effectively. There is a critical need to improve the sharing of threat intelligence across the federal government, with key American allies, and in an appropriate but collaborative way with tech companies that often are cybersecurity first responders. This also

requires consideration of new measures to ensure that attacks on private enterprises are reported in an appropriate way to a federal agency, consistent with the protection of personal privacy.

4. Are there particular criteria the Department could issue to inform utility procurement policies, state requirements, or FERC mandatory reliability standards to mitigate foreign ownership, control, and influence risks?

With respect to investments in Cloud Computing, the Department should work to enable utility procurements for cloud computing resources that bring greater security and opportunity for electric utilities. Specifically, providing guidance to state utility commissions on allowances for regulated utilities to capitalize investments in cloud computing will remove the current disincentives for investments. Utilities are generally allowed to earn a return on their capital investments – and therefore have a natural incentive to invest in on-premises computing. On the other hand, cloud computing is often viewed as a service that is recovery as operations and maintenance, which is not subject to a return. DOE should encourage state regulators to review and revise their rules to create a level playing field for investment in cloud computing options for regulated utilities.

Recently, (December 17, 2020) Federal Energy Regulatory Commission (FERC) issued an order directing informational filing to North American Electric Reliability Corporation (NERC) towards virtualization and cloud computing services that address the virtualization and data storage of Bulk Electric System (BES) and Building Component Safety Information (BCSI) data by clarifying their compliance treatment in the Critical Infrastructure Protection (CIP) Reliability Standards. The commission may use the scheduling order and notice of inquiry to determine whether it would be appropriate to direct NERC to develop modifications to the CIP Reliability Standards to facilitate the voluntary adoption of virtualization and cloud computing services by registered entities. DOE should encourage FERC and NERC towards adoption of cloud services that can leverage public-private partnerships to develop new robust cybersecurity tools while leverage the scalability of cloud computing that will be necessary for the energy transition to low carbon power generation and broad scale electrification.