COMPLIANCE BRIEF: NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY'S FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

OVERVIEW

On February 2013, President Barack Obama issued an Executive Order 13636, Improving Critical Infrastructure Cybersecurity. The Executive Order is directed at the **National Institute of Standards and Technology (NIST)** to work with stakeholders to develop a *voluntary framework* – based on existing standards, guidelines, and practices - for reducing cyber risks to critical infrastructure. On February 12, 2014, NIST released the first version of the Framework for Improving Critical Infrastructure Cybersecurity. The Framework, created through collaboration between technologists and the government, consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the Framework helps owners and operators of critical infrastructure to manage cybersecurity-related risk.

Practitioners should keep in mind that the Framework is an overall structure that can be addressed by different security standards, including, for example, NIST 800-53, ISO 270001, and COBIT 5.

National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity and Varonis

The following is a table containing sections of NIST's Cybersecurity Framework and an explanation describing how Varonis solutions can help reduce security risks and protect an organization's computer infrastructure:

NIST's Cybersecurity Framework	**Description**	**Varonis Solutions**
Identify: Asset Management The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried	
	ID.AM-2: Software platforms and applications within the organization are inventoried	
	ID.AM-3: Organizational communication and data flows are mapped	DatAdvantage shows all directory and file share contents mapping users to data and vice versa
	ID.AM-4: External information systems are catalogued	
	ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	Varonis provides the ability to classify data based on business guidelines and ensure that proper controls are in place based on that classification.
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	

Identity: Business Environment The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.		The Varonis Operational Plan is a methodology for implementing the Data Governance Suite. As it is a methodology describing a sequence of operations, techniques, and reports to run in order to take unstructured data from its natural, "uncontrolled" state, to a governed state.
Identity: Governance The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.		Varonis can ensure that only business owners manage data authorizations, and further allow auditors and compliance personnel to monitor the process
Identity: Risk Assessment The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.		Varonis significantly reduces the risk of data loss and misuse by continually maintaining access controls that are restrictive to business need to know
Identity: Risk Management Strategy The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders ID.RM-2: Organizational risk tolerance is determined and clearly expressed ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical	Varonis products can help quickly identify operational risk with regard to file system, email, and SharePoint data. DatAdvantage will report on data which has weakened security through global groups (everyone,

	infrastructure and sector specific risk analysis	authenticated users, etc.) or otherwise excessive access, as well as users and groups which have excess access
Protect: Access Control Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	PR.AC-1: Identities and credentials are managed for authorized devices and users	Varonis allows the enforcement of an access control policy by ensuring that business owners accept or reject recommendations for permissions revocations
	PR.AC-2: Physical access to assets is managed and protected	Varonis can help monitor and audit third-party system activity on unstructured and semi structured data
	PR.AC-3: Remote access is managed	DatAnywhere instantly enables mobile access, file synchronization, and secure 3rd party sharing for your existing file shares. Files can stay exactly where they are—on existing SMB file servers or NAS. Third party access is monitored and can be revoked at any time. Third party links can contain expiration dates and pin codes for extra security and can be revoked at any time. Third parties do not require an entry in the organizations Active Directory or LDAP system. Private cloud benefits: • Definitive copies of files are always stored on corporate storage • No one gets permissions to shared data unless they already have it • Users authenticate to Active Directory or LDAP and there is no need to reconfigure or replicate permissions

		• IT controls speed, availability, and security
	PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	Varonis helps organizations comply with initiatives to ensure least privilege access to regulated data. The system analyzes data access patterns and continually recommends that those without business need to data have their privileges revoked
	PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	
Protect: Awareness and Training The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.		Varonis staff are also avid learners and educators. Here are some of the educational opportunities we offer and provide: • Professional Services: ensures our customers can effectively use the product to fulfill all their use cases and to use our products. • Varonis Blog: learn more about security, privacy, IT Operations and more on our blog. We post approximately 3-4 blog posts per week • Office Hours: 1 free hour one-on-one live web session with your local Engineer to discuss operational and security questions.
Protect: Data Security Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality,	PR.DS-1: Data-at-rest is protected	**Confidentiality** To ensure that information and records, especially sensitive data remains confidential and unpublished, organizations can implement the

integrity, and availability of information.		Varonis IDU Classification Framework. It helps identify sensitive content within records, determine who has access to it, who is using it, and who should be responsible (data owners) – all of which are also reportable. **Integrity and Availability of Information** Varonis ensures the success of audits and examinations and can demonstrate effectiveness of security, operational integrity in a number of ways: • Varonis recommends the revocation of permissions to data for those users who do not have a business need to the data – this ensures that user access to data is always warranted and driven by least privilege • Varonis generates reports showing the history of permission revocations and the percentages by which overly permissive access was reduced • Varonis DataPrivilege provides a mechanism via a web-based application by which to monitor, administer (allow/deny) all access requests to unstructured data. Requestors, data owners, technical controllers, financial

		controllers are all united in communication and action through this system. With regard to requests to access unstructured data on file shares, all actions taken and rationale for them are recorded. Further, a workflow is enforced (i.e. requests to financial folders go straight to the business owner). Via these capabilities, entities can demonstrate a historical and sustained enforcement of least privilege access and its effects.
	PR.DS-2: Data-in-transit is protected	
	PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	**Stale Data** Varonis DatAdvantage keeps an audit trail of every open, create, move, modify and delete on the file system. By analyzing this data over time, Varonis can quickly identify which files and folders are no longer in use. **Unused Users and Groups** Varonis combines user and group information from directory services, permissions information on file and SharePoint servers, and a complete audit trail of all file activity. This means that DatAdvantage can quickly identify which users and security groups are no longer in use, meaning

		they can be safely removed without affecting business process. **Data Transfers** Data Transport Engine provides the flexibility to configure complete end-to-end migration rules: define source criteria based on path, and/or content, classification rule, Varonis ownership and follow-up (flag/ tag) criteria, define destination path, folder, and permissions translation, and when the migration will take place. The ability to configure these rules allow for the rapid and safe execution of complex data migrations, and to easily implement and enforce policies for data retention and location based on content, accessibility, and activity.
	PR.DS-4: Adequate capacity to ensure availability is maintained	
	PR.DS-5: Protections against data leaks are implemented	
	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	
	PR.DS-7: The development and testing environment(s) are separate from the production environment	
Protect: Information Protection Processes and Procedures	PR.IP-1: A baseline configuration of information technology/industrial	DatAlert can be configured to send real-time alerts on a number of actions

Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	control systems is created and maintained	including the granting of administrative rights to a user or group. It baselines every user's normal access behavior and can generate real time incident response when behavior becomes abnormal.
	PR.IP-2: A System Development Life Cycle to manage systems is implemented	
	PR.IP-3: Configuration change control processes are in place	Varonis DatAdvantage monitors every user's file touch and stores in a searchable format, all aspects of data use for information stored on file servers and Network Attached Storage (NAS) devices. Varonis DatAlert can alert when in real time when inappropriate activities take place (changes made outside change control windows, etc.)
	PR.IP-4: Backups of information are conducted, maintained, and tested periodically	
	PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	
	PR.IP-6: Data is destroyed according to policy	
	PR.IP-7: Protection processes are continuously improved	

	PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	
	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	
	PR.IP-10: Response and recovery plans are tested	
	PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	
	PR.IP-12: A vulnerability management plan is developed and implemented	
Protect: Maintenance Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	
	PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	Varonis gives the means to conduct a full in depth data entitlement review by which all user privileges to data is reported. It also provides reports of historical access rights to data sets showing any trends toward overly permissive access
Protect: Protective Technology Technical security solutions are managed to ensure the security	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	DatAdvantage can help organizations identify the use of privileged access accounts and ensure that appropriate segregation of duties is implemented

and resilience of systems and assets, consistent with related policies, procedures, and agreements		through best practices as they relate to use of separate administrative accounts. In addition to the visibility provided through our Log, Statistics, and Reports features, DatAlert can be configured to notify administrators when elevated accounts have been used or when an account has been elevated in group membership to an administrative level. Such controls are key to securing the environment, and our reporting capabilities can play a critical role in maintaining the data's lifecycle through regular audits and report subscriptions.
	PR.PT-2: Removable media is protected and its use restricted according to policy	
	PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	
	PR.PT-4: Communications and control networks are protected	
Detect: Anomalies and Events Anomalous activity is detected in a timely manner and the potential impact of events is understood.	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	**Data breaches and Monitoring** Varonis DatAlert provides real-time alerting based on file activity, Active Directory changes, permissions changes, and other events detected by Varonis DatAdvantage. Alert criteria and output are easily configurable so that the right people and systems can
	DE.AE-2: Detected events are analyzed to understand attack targets and methods	

	DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	be notified about the right things, at the right times in the right ways. DatAlert improves your ability to detect possible security breaches and misconfigurations, and the audit trail in DatAdvantage provides valuable information during the incident response process.
	DE.AE-4: Impact of events is determined	
	DE.AE-5: Incident alert thresholds are established	
Detect: Security Continuous Monitoring The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-1: The network is monitored to detect potential cybersecurity events	Recently we published an article to our blog about a how a Varonis customer used DatAdvantage to quickly and effectly isolate and halt the spread of the Cryptolocker virus in their environment. To quote our customer, "Within DatAdvantage I ran a query on that specific user and realized that there were over 400,000 access events that had been generated from that user's account. It was at that point that we knew it was a virus... Once we had identified the second user, we went back to DatAdvantage to identify the files they had accessed. There were over 200,000 access events generated from this user's account." The fact that they were able to quickly identify which files had been corrupted helped them reduce the impact of the virus on the environment and the downtime for the users. In addition, it allowed them to maximize their time
	DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	
	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	
	DE.CM-4: Malicious code is detected	
	DE.CM-5: Unauthorized mobile code is detected	
	DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	
	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	
	DE.CM-8: Vulnerability scans are performed	

		and resources by only having to restore the data that was affected. To read more about this success story, check out: http://blog.varonis.com/datadvantage-can-help-recover-virus/
Detect: Detection Processes Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	DataPrivilege helps organizations not only define the policies that govern who can access, and who can grant access to unstructured data, but it also enforces the workflow and the desired action to be taken (i.e. allow, deny, allow for a certain time period). This has a two-fold effect on the consistent and broad communication of the access policy: • it unites all of the parties responsible including data owners, compliance officers, auditors, data users AND IT around the same set of information and • it allows organizations to continually monitor the access framework in order to make changes and optimize both for compliance and for continuous enforcement of warranted access.
	DE.DP-2: Detection activities comply with all applicable requirements	
	DE.DP-3: Detection processes are tested	
	DE.DP-4: Event detection information is communicated to appropriate parties	
	DE.DP-5: Detection processes are continuously improved	
Respond: Communications Response activities are coordinated with internal and external stakeholders, as appropriate, to include external	RS.CO-1: Personnel know their roles and order of operations when a response is needed	
	RS.CO-2: Events are reported consistent with established criteria	Varonis provides highly detailed reports including: data use (i.e. every user's every file-touch), user activity

support from law enforcement agencies.		on sensitive data, changes including security and permissions changes which affect the access privileges to a given file or folder, a detailed record of permissions revocations including the names of users and the data sets for which permissions were revoked.
	RS.CO-3: Information is shared consistent with response plans	
	RS.CO-4: Coordination with stakeholders occurs consistent with response plans	
	RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	