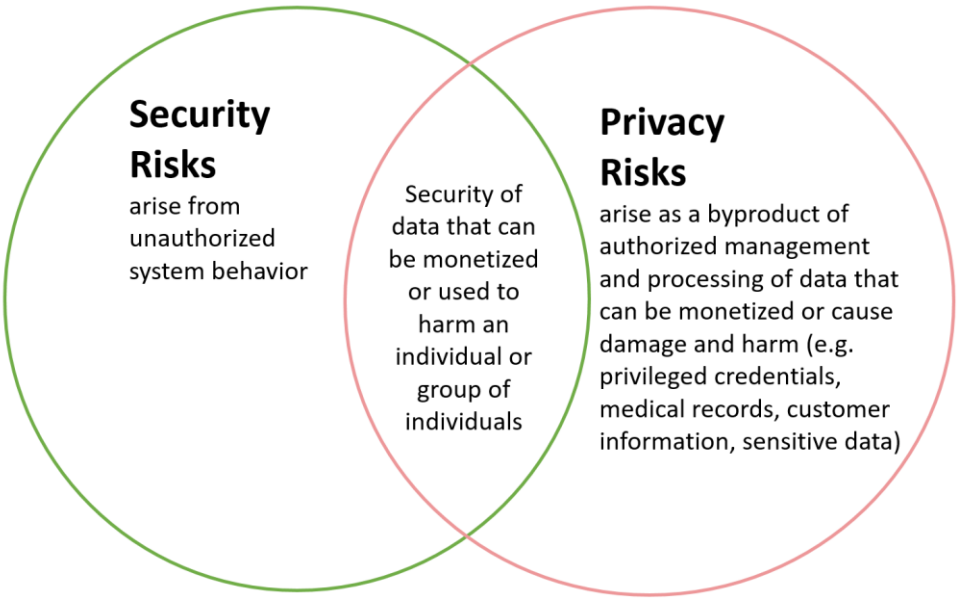
# One Identity RFI response for the NIST Privacy Framework

One Identity submits the following two recommendations in response to the NIST Privacy Framework Request for Information (RFI).

## Expand the Security and Privacy Risk Relationship (Slide 11) beyond PII data

Privacy risks are expanding exponentially as data banks grow, bad actors find new access points, and dark consumers (i.e. black markets, competitors, political foes) identify new ways to aggregate and manipulate pilfered data.

Currently, **Slide 11** acknowledges that individual privacy cannot be achieved solely by securing PII, yet, PII is the center focus. The following slide, center section, expands the scope from PII to data that can be monetized or used to harm an individual or group of individuals. PII information is one of many types of private data. The section on the right, **Privacy Risks**, expands the definition and provides examples. The examples include privileged credential data (i.e. highly secure log on credentials) and various types of sensitive data, which includes PII, that could be used to target groups of individuals for financial gain or to harm.




This expanded scope of private data is needed to thwart the following types of scenarios where data can be stolen or handled irresponsibly so that private data is used for financial gain or harm.

- Theft of authentication credentials, especially credentials with privileges which can lead to harm of the holder of the credentials (e.g. security personnel) or be the cause of unauthorized data alteration or disclosures.
- Theft of system logs which are indicators of the state of the system infrastructure and inevitably hold private data that can be monetarized or cause harm. System logs are often handled in unsecured processes but should be protected like any other repository. System logs should be secured while in transit and at rest.
- Theft of private data used for personal manipulation (e.g. clinical information, contact information, claims information, customer lists, or sensitive emails).
- Theft of private data used for political manipulation (e.g. voting history, discrimination issues, or false fact dissemination).
- Theft of private data used for social harm to manipulate personal opinion or target individuals in groups (e.g. targeting of individuals meeting certain social standing, social views, or are engaged in social movements).
- Theft of private data used for monetary gains (e.g. theft of cardholder data, financial records).
- Placement of malware to inhibit or halt system functions for a single or targeted group of individuals (e.g. prohibiting certain individuals for applying for goods or services or gaining accesses).
- Placement of ransomware to charge a fee to return private data and Cisco estimates ransomware attacks are growing more than 350 percent annually. Source

## Target the privacy exposures from unsecured privileged accounts

Privileged accounts are high risk points for privacy breaches.

In a recent study of 1000 security professionals, most security personnel could steal data and a surprising number would steal data. Dimensional Data found that 77 percent of security personnel admitted, if they were leaving their organization, they could easily steal data. An additional 12 percent of respondents admitted that, if they were disgruntled with their organization, they would steal data. Many privileged users have virtually unlimited access to data that, if stolen, constitutes a severe privacy breach. Source

In a 2017 report, industry analyst house Forrester Research estimated that 80 percent of security breaches involve privileged credentials that typically belong to the IT professionals who administer the systems, databases, and networks of an organization. Source

NIST's Privacy Framework must include solid privileged account management (PAM) scenario that includes the following best practices and tools.

### Privileged account access best practice

NIST's Privacy Framework must recommend that organizations control, monitor, and audit privileged access to prevent attacks from insiders with valid access, insiders with improperly

escalated access, and bad actors inside or outside the organization that have stolen privileged access credentials. This includes frequently deploying discovery tasks to fully discover all privileged accounts and:

- Validate who has each level of access to sensitive and mission critical data.
- Validate who has administrative control of the networks.
- Ensure employees or contractors have the minimum privileges required.
- Shutdown unknown privileged accounts quickly.

Organizations must limit of granting privileged credentials by role, profile, and timed availability on hardened appliances for maximum security.

Possible tool: One Identity Safeguard for Privileged Passwords

### Privileged account activity monitoring best practice

NIST's Privacy Framework must propose that organizations record activities during every privileged access session, identify inappropriate behavior, and ensure timely and appropriate incident response. Organizations must use available technology to monitor privileged sessions to prevent intended privileged account misuse, unintended employee negligence exposing risk, facilitate privacy compliance, and accelerate forensics investigations. Using session recordings, organizations can increase the detection of criminal and irresponsible behaviors, have solid evidence to enforce corrective actions and penalties, and increase the likelihood of being caught as a deterrent.

Possible tool: One Identity Safeguard for Privileged Sessions

### Privileged account misuse prevention best practice

NIST's Privacy Framework must advocate that organizations quickly detect breaches to thwart misuse and stop the extent of harm. Organizations need to implement tools that integrate session's data and use machine learning algorithms in real time comparisons of actual user activity to user behavior. Anomalies are detected real time and are ranked based on risk to prevent data breaches. Alerts immediately report suspicious activity enabling the organization to proactively take steps to block, quarantine, and review actions. These tools provide organizations an unprecedented opportunity to immediately shut down users engaged in irregular privileged access behavior patterns. Further, the organization can take steps to investigate behavior patterns, unanticipated points of system exposure, and implement preventative measures to avert future incidents thus heightening overall security.

Possible tool: One Identity Safeguard for Privileged Analytics

# Target the privacy exposures from governance failures

### Data governance best practices

When it comes to securing data that can be monetized or used to cause damage and harm, it is essential to decide who gets access and to ensure least access is granted to protect private data. In order for processes to operate on an optimal level, policies must be established to mass manage access and activities on an organizational level, typically by grouping users based on roles.

NIST's Privacy Framework must include solid Identity and Data Governance scenarios that includes the following best practices:

- Restricted access: The capability to ensure that sensitive, unstructured data is only accessible to approved users by defining access policies.
- Classification of data: The ability to classify governed data manually, allowing access to authorized individuals.
- Access request and validation: The ability to monitor access requests and validations. Implement a recertification process where data owners verify and attest employee access.

Possible tools: One Identity Safeguard for Privileged Passwords and One Identity Safeguard for Privileged Sessions.

# Target the privacy exposures from system log exposures

### Log data best practices

NIST's Privacy Framework must include securing system logs which are used as a means to enhance security and typically include private data that can be monetarized or cause harm. Processes involving system logs must be secure and ensure data is secure in transit and at rest.

The following example shows the type of private log on information found in log messages including the user ID and IP address. This data can be useful to useful to malicious actors and discoverable by scanner bots.

```
Apache login log:

122.174.58.199 10080 - S_Miller [18/Oct/2014:02:00:01 +0100] "GET
/isbin/INTERSHOP.static/WFS/EKI-PK-Site/EKIPK/
uk_UK/images_themenseiten/internet/extras/internet_extras/hotspot/wlantogo/images/
button_grau_links.png HTTP/1.1" 304 - "X-Hitnet=-"

User IP: 122.174.58.199

User name: S_Miller

Geo location and timezone: UK / GMT +0100
```

To secure sensitive data in system log messages, NIST's Privacy Framework should call for the following system log security measures.

- Log data minimization: Restrict the accessibility to PII and other sensitive data within a log to a necessary minimum. Use log parsing and filtering to decrease data visibility in log information to only that data that is required by the end user.
- Data masking**:** Hide PII and other sensitive data in logs from plain sight by encrypting only those data segments. This is best accomplished by anonymization to either encrypt or remove sensitive data in the log messages allowing the logs to be secure both while in transit and at rest. Anonymization protects privacy via irreversibly de-identifying data.
- Log pseudonymization**:** Create two logs. One log version has obfuscated hashed data values and is suitable for audits due to the consistency of obfuscated data replacement. The other log version is completely encrypted for processing and analysis. Log pseudonymization is achieved by properly parsing and rewriting logs. The risk is that the data can potentially be reidentified with the use of additional information.
- Preventative measures: Set up blacklists and isolated and monitored honeypots including spamtraps.

Possible tool: Log management technologies such as syslog-ng.

### About One Identity

One Identity, a Quest Software business, helps organizations get identity and access management (IAM) right. With a unique combination of offerings including a portfolio of identity governance, access management and privileged management, and identity as a service that help organizations reach their full potential, unimpeded by security yet safeguarded against threats. One Identity has proven to be a company unequalled in its commitment to its customers' long-term IAM success. More than 7,500 customers worldwide depend on One Identity solutions to manage more than 125 million identities, enhancing their agility and efficiency while securing access to their data -- wherever it might reside. For more information, visit http://www.oneidentity.com.