In 2011, U.S. Executive Order 13587 established the National Insider Threat Task Force (NITTF), under joint leadership of the Attorney General and the Director of National Intelligence. A year later, the President issued the National Insider Threat Policy. This policy introduced a set of standards - including people, process, and procedures - for preventing damage from insider threats, i.e. malicious or harmful-but-inadvertent activities by employees or contractors with trusted access to sensitive data and system. This brief describes how the Exabeam Security Intelligence Platform supports the National Insider Threat Policy and its components.

The National Insider Threat Policy (NITP) requires agencies to establish an integrated capability to monitor and audit information for insider threat detection and mitigation. Program requirements include the ability to monitor user activity on classified computer networks controlled by the Federal Government and to gather and centrally analyze, report, and respond to insider threats. The Policy is broad and addresses many dimensions of a comprehensive insider threat program. Since some of these dimensions (for example, establishing new roles and assigning people to those roles) are not related to a technology solution such as Exabeam, they are not addressed here.

The ITTF established multiple standards for implementing an insider threat program. Standards relevant to Exabeam are listed below.

**NITP Standards: Information Integration, Analysis, and Response**

The NITP standards require Agency heads to:

- Build and maintain an insider threat analytics and response system that can process information from CI, Security, IA, HR, user activity, and other information.
- Create procedures for investigating and resolving insider threat matters, while supporting centrally-managed response actions.
- Develop procedures for documenting each insider threat reported and response action taken.

**NITP Standards: Monitoring User Activity on Networks**

The NITP standards require Agency heads to ensure that insider threat programs include:

- The ability to monitor user activity on all classified networks in order to detect activity indicative of insider threat behavior.
- SLAs defining how behavior will be identified and reported to subscriber personnel.
- Procedures for protecting and limiting access to user activity monitoring methods and results to authorized personnel.

As a technology solution, the Exabeam Security Intelligence Platform supports and enables Agencies to meet each of the above standards.
Exabeam Overview: Security Intelligence for Insider Threat Management

Exabeam offers a comprehensive security intelligence platform, built from the ground up on modern technologies, that delivers advanced detection, analytics, and response capabilities. This platform includes five key components, each of which can be purchased and deployed separately or as a complete solution:

**Exabeam Data Lake** - Exabeam Data Lake operates at lightning-fast speeds and can be scaled far beyond the capabilities of legacy log management technologies. Since Data Lake was designed for security log management, it includes context-aware capabilities that improve ease of use for security analysts. For example, Data Lake formats log records based on their types, highlighting the most relevant fields for easy visual scanning.

In addition to world-class speed and scalability, Data Lake is licensed (and priced) in a way that acknowledges the underlying open source technology. Unlike legacy log management systems, Exabeam Data Lake is not priced based on data volumes or EPS, so customers can capture, store, and search as much data as they wish. Costs are predictable and not a barrier to analyzing as much data as an organization might need to perform effective detection and reporting.

**Exabeam Cloud Connectors** - In addition to the log collection agents included in the Elastic Stack, Exabeam offers log collectors for the most popular cloud services, including Salesforce.com, Box, Office365, and others. Exabeam Cloud Connectors provide an easy way to report and analyze users’ cloud activity and behavior, integrated with activity across internal systems.

**Exabeam Advanced Analytics** - Already the #1 most-deployed User and Entity Behavior Analytics solution in the world, Exabeam Advanced Analytics detects insider threats, compromised accounts, and data loss via deep learning and specialized statistical risk models. The Exabeam behavioral analytics capabilities recreate the entire attack chain, piecing together both normal and anomalous behavior of users and entities. Based on a patented session data model, Exabeam creates, in seconds, automatic incident timelines that show all activity - good and bad - across multiple IP addresses, devices, and credentials. Exabeam analytics amplifies the abilities of SOC and IR staff by automating the manual drudge work of creating investigation timelines.

**Exabeam Threat Hunter** - Where behavioral analytics uses machine learning techniques to notify an analyst about an emerging threat, Exabeam Threat Hunter enables that analyst to proactively identify threats on the corporate network. Using a simple checkbox interface, Exabeam Threat Hunter can find all user or machine sessions that match any combination of attributes and activities. Analyst can easily pivot and drill down into sessions to follow attacks. This capability is easily performed by even new, Tier 1 analysts.

**Exabeam Incident Responder** - When Exabeam detects an insider threat or other incident, the job isn’t completed. Now your organization must respond efficiently and effectively. Exabeam Incident Responder automates a firm’s response procedures with incident workflows and playbooks. Incident Responder ships with a set of pre-built playbooks for the most common incident types, such as malware alerts, phishing incidents, data loss alerts, departed insider issues, etc. Playbooks can be modified, and customers can create their own playbooks, as well.
Mapping Exabeam Functions to NITP Standards

Exabeam provides technology solutions to support the standards listed in the previous section:

<table>
<thead>
<tr>
<th>NITP Standard</th>
<th>Exabeam Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Build an insider threat analytics system that can process information from CI, Security, and other information sources</td>
<td>Exabeam can ingest any type of activity information, parse it into a data model for insider threat detection, and positively connect that activity to an identity. With over 1,000 data parsers available out of the box, Exabeam can analyze most common data feeds upon installation. Any new feeds are typically added within 24 hours.</td>
</tr>
<tr>
<td>Create procedures for investigating insider threats, with centrally managed response</td>
<td>Exabeam automatically creates insider threat investigation timelines, showing all activity, why that activity is or isn’t risky, and whether it’s happened before. Timelines feed automatic response capabilities, which can be managed in a centralized manner.</td>
</tr>
<tr>
<td>Document insider threats and responses taken</td>
<td>Investigation timelines provide a detailed record of every action taken by an insider, related to an insider threat. Timelines include insider actions that span multiple account IDs, devices, IP addresses, networks, etc. In addition, Exabeam’s incident response capabilities provide a related documentation of every response action taken relative to the insider threat. Auditors can use Exabeam to show everything a particular insider has done within any window of time.</td>
</tr>
<tr>
<td>Monitor user activity on all classified networks to detect insider threats</td>
<td>Exabeam uses a combination of machine learning, data reconstruction, and risk modeling to determine which users are acting in a unusual and risky manner. Risk scoring occurs in near-real time, so that analysts can take action to prevent breaches.</td>
</tr>
<tr>
<td>Define how behavior is identified and reported</td>
<td>Unlike other behavioral analytics systems, Exabeam provides plain-English descriptions of every identified risky action, including whether it’s happened before, whether any peer of the insider has performed the action, why it’s risky, etc.</td>
</tr>
<tr>
<td>Protect and limit access to methods and results to authorized personnel</td>
<td>With both role-based access control and data masking, Exabeam automatically limits who can see methods and results. Masking enables analysts to detect insider threats without showing the actual user or affected-system names. Results can be unmasked based on policy and specific administrative action.</td>
</tr>
</tbody>
</table>
World-Class, Proven Insider Threat Detection and Response

The Exabeam Security Intelligence Platform has been deployed enterprise-wide at over 200 leading government, commercial, and critical infrastructure organizations in the past 12 months. The platform provides a complete solution for collecting unlimited insider activity information, analyzing it to detect unusual and risky behavior, and responding in a secure, repeatable and auditable manner.

As insiders begin to perform actions that are both unusual and risky, Exabeam presents these, in real time, in a coherent timeline. The timeline presents all actions, both good and bad, even as the insider changes accounts, devices, networks, IP addresses, etc. Timelines provide instant context so that analysts understand exactly what is happening and why it is risky.

When an insider event is detected and confirmed, Exabeam’s incident response capability enables automatic or manual execution of pre-built playbooks, designed to codify agency policy and industry best practices. The overall result is faster and more accurate threat detection, plus consistent and effective threat response.

Insider incident timelines are automatically constructed in order to facilitate quick investigations.

ABOUT EXABEAM
Exabeam’s user and entity behavior analytics solution leverages existing log data to quickly detect advanced attacks, prioritize incidents and guide effective response. The company’s Stateful User Tracking™ automates the work of security analysts by resolving individual security events and behavioral anomalies into a complete attack chain. This dramatically reduces response times and uncovers attack impacts that would otherwise go unseen. Built by seasoned security experts and enterprise IT veterans from Imperva, ArcSight and Sumo Logic, Exabeam is headquartered in San Mateo, California and is privately funded by Aspect Ventures, Icon Ventures, Investor Shlomo Kramer, Lightspeed Venture Partners, and Norwest Venture Partners.

For more information, please contact info@exabeam.com