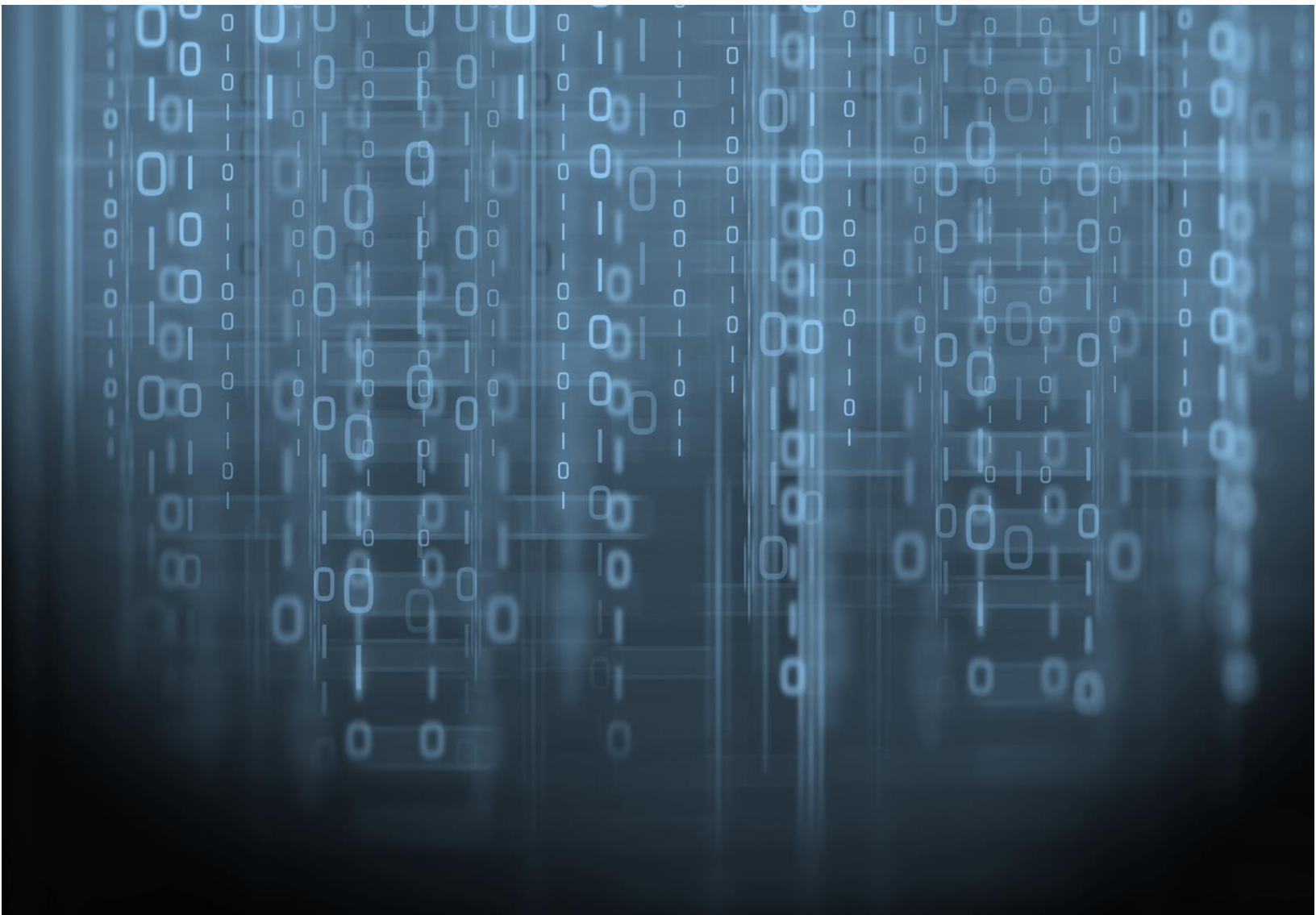
May 2017

BEYOND PROVISIONING:

Leveraging Identity Governance and the 5 A's to Optimize Business Functions, Security, and Compliance in Federal Agencies



CONTENTS:

INTRODUCTION

A common theme exists among the most devastating Federal cyberattacks of the last five years: all have resulted from inadequate Identity and Access Management (IAM) controls. Whether launched by outsiders—like the massive 2015 breach of the Office of Personnel Management (OPM)—or perpetrated by insiders like Chelsea Manning and Edward Snowden, each attack involved the exploitation of inadequate identity controls to steal valuable data, endanger employees, and harm the U.S. government. In the private sector as well, the most damaging, headline-grabbing cyberattacks of the last five years—think Target, Anthem, Sony, JP Morgan Chase, the DNC, and Home Depot—have had one thing in common: identity as their vector of attack.

In 2016, the U.S. Commission on Enhancing National Cybersecurity addressed this problem head-on, noting in its report that "Identity, especially the use of passwords, has been the primary vector for cyber breaches—and the trend is not improving despite our increased knowledge and awareness of this risk." The report went on to lay out "an ambitious but important goal" for the incoming Trump Administration: "to see no major breaches by 2021 in which identity…is the primary vector of attack."

Achieving this goal in the U.S. government will, in large part, require agency adoption of modern IAM systems that not only deliver strong authentication, but also take a holistic approach to managing the full lifecycle of identity. Yet today, we see many agencies clinging to archaic, first-generation IAM systems that focus largely on automating the provisioning of accounts, without also addressing the more important issue of identity governance. This paper serves to highlight the cybersecurity risks posed by Federal reliance on IAM solutions that fail to go beyond basic account provisioning, and lays out the case for the adoption of more comprehensive identity governance platforms.

Designed to facilitate IT automation and create operational efficiencies, provisioning solutions alone fail to achieve what has become the key use case driving IAM adoption today: security. Governance platforms not only offer the same automated credentialing functionality as traditional provisioning tools, but also assist agencies in navigating the federal regulatory environment, including compliance with Federal Information Security Management Act (FISMA) and Federal Identity, Credential, and Access Management (FICAM) policies.

As The Chertoff Group noted in a white paper published last year, true identity security requires a holistic approach to IAM, rooted in governance, that delivers strong Authentication in addition to Authorization, Administration, Analytics, and Audit capabilities. An IAM approach that goes beyond basic provisioning to deliver the "Five A's" of identity management not only enhances security and eases compliance, but also drives operational efficiencies and business transformation. Identity becomes the great enabler.

This white paper will articulate the differences between traditional provisioning and superior identity governance solutions and explain how governance platforms facilitate compliance with federal regulations including FISMA and FICAM. The paper will also lay out how agencies have a unique opportunity in 2017 to leverage the Department of Homeland Security's (DHS) Continuous Diagnostic and Mitigation (CDM) program to acquire a more comprehensive IAM solution.

TRADITIONAL FEDERAL PROVISIONING VS. IDENTITY GOVERNANCE

Modern-day identity governance has its roots in legacy user administration and provisioning. Early provisioning-only solutions were developed to automate the process of adding, modifying, and deleting user accounts for IT operations—alleviating the administrative burden and user pain associated with maintaining multiple account repositories. When new financial regulations forced SEC-registered corporations to provide more visibility into their internal controls, however, the provisioning tools thought to provide great operational efficiencies proved insufficient for security and compliance purposes. Likewise, the increasing sophistication of identity-centric attacks against Federal systems has made clear that legacy provisioning systems are no longer sufficient.

Provisioning tools fail on several accounts to address security and compliance needs.

	PROVISIONING-ONLY SOLUTIONS	GOVERNANCE PLATFORMS
 COST	The cost and complexity of implementing legacy provisioning solutions can limit deployment across agencies. Enterprises with hundreds or thousands of systems and applications to provision may find the tools prohibitively expensive and opt to pick and choose which dozen or so applications to target. The limited view afforded in this model, though less operationally burdensome than manual controls, is not sufficient to meet enterprise-wide visibility and control requirements.	Identity governance solutions gather technical identity data scattered across multiple enterprise systems and consolidate the information into a centralized business information repository. The centralized repository containing log and identity information can be aggregated and scaled at no additional cost, sparing agencies from having to pick and choose which applications to provision and providing fuller coverage at a better dollar value.
 GRANULARITY	Most provisioning systems are designed to manage account-level access. They do not provide the visibility into granular application entitlements and permissions needed to manage insider risk and privilege escalation. Without this level of detailed application entitlement information, provisioning systems fail to enforce access policies and evaluate privilege creep.	Among the significant innovations offered by governance products is the ability to view and consider access decisions at a more granular level. Provisioning systems offer some functionality around access decisions, but are generally limited to a coarse-grained view focused at the application level; they fall short when asked to deliver answers to the more fine-grained question of “who can do what within each application?” Governance solutions go deeper—lifting the curtain to reveal the specific privileges users possess, and providing interfaces that allow administrators to more easily monitor and adjust theses privileges as roles or attributes change.

	Provisioning solutions cater to technical users, such as IT operations staff and administrators. They do not translate information well for non-technical user populations like audit and compliance.	Governance solutions translate technical identity data into business information, enabling users to filter and interpret entitlement data according to overall risk and business policies. By providing a fine-grained view of entitlements, overlaid with business processes and workflows, governance platforms make identity data accessible to its various consumers—technicians, auditors, and executives alike.

Many federal agencies are under the false assumption that they are protected if they have implemented provisioning administration solutions as outlined in federal directives like HSPD-12, FICAM, and DOD 8500. The truth is that despite their administrative benefits, the technical limitations of provisioning solutions place organizations at risk of security breaches and failed IT audits.

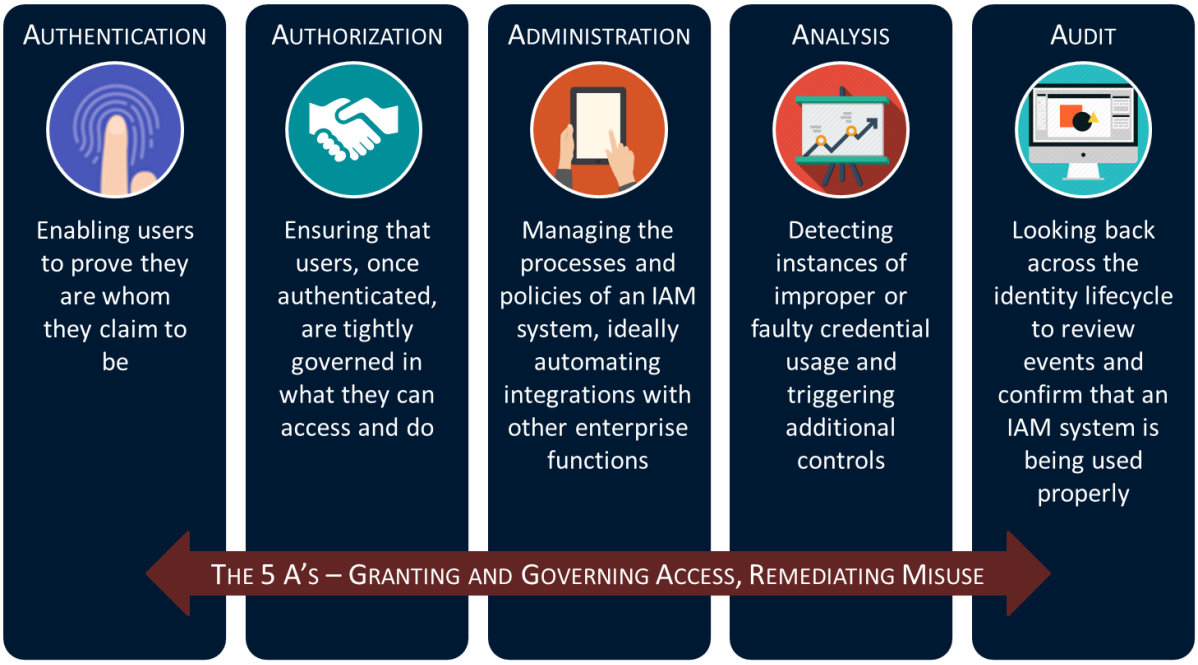
To mitigate these risks, organizations need to adopt an enterprise-wide view of entitlements and access privileges based on what actions a user can and should be able to perform within a given business application environment. Identity governance solutions do just that, addressing the specific issues of governance, risk management, and compliance in the identity management space.

A properly-configured governance platform can not only address the core issues associated with provisioning tools, but also help reduce cybersecurity exposure and costs and provide additional operational, compliance, and risk management benefits.

Beyond providing a credential management function and addressing the technical shortcomings of legacy provisioning tools, governance platforms provide superior risk management and cybersecurity defenses. Provisioning-only tools do not mitigate threats within a network—threats posed by legitimately-credentialed insiders. Nor do they mitigate threats from external attackers who have compromised a credential. Addressing these threats properly requires a more rigorous approach to IAM that addresses each of the Five A's.

IDENTITY GOVERNANCE AND THE FIVE A'S

To truly address the full range of risks to Federal systems tied to identity, agencies should take a holistic approach to identity security—one rooted in governance. The Chertoff Group views the IAM lifecycle through the prism of "The Five A's"—which, when tackled together, cover the full range of identity risks:



Properly implemented, this governance-based approach enables agencies to answer a number of critical questions around identity security, including: Beyond these three categories, however, there is another way to split authentication technologies:

- How is a credential provisioned?
- How are users authorized to access data or resources?
- How are those authorizations managed and updated as roles or attributes change?
- How is access to privileged systems provisioned and managed?
- Are Privileged Account Management (PAM) solutions tightly integrated with the rest of the IAM stack?
- Are firm controls in place to prevent the creation of new "phantom" accounts?
- How is access revoked when someone leaves an organization, ensuring that "orphan" accounts do not persist?
- With a blended workforce of employees and contractors – including some that may not have a PIV card – how are access and privilege consistently managed through a unified approach?

Governance solutions address insider risk by assigning employee risk profiles and automatically flagging privilege escalation requests to deter inadvertent or intentional access to restricted networks without proper authorization. Governance limits the extent to which identity offers a vector of attack within a network by controlling user access privileges across multiple systems and ensuring that negligent and disgruntled insiders are unable to access—and therefore leak or compromise—information outside their purview. A strong identity governance solution will also generate risk scores for all users based on their combined entitlements and historical performance.

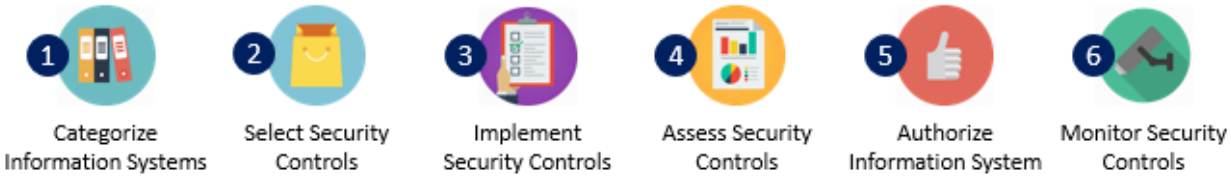
GOVERNANCE AND ITS BENEFITS TO AUDIT AND COMPLIANCE

Beyond their benefits to security and operations, governance platforms help organizations define and enforce user access policies, such as separation-of-duty (SoD), and automate the process of reviewing user access rights across the organization by initiating campaigns for business managers to approve or revoke access as part of a centralized governance program. These processes greatly ease compliance requirements applicable to federal agencies, including FISMA and FICAM.

FISMA

The Federal Information Security Modernization Act of 2014 amended and updated the Federal Information Security Management Act of 2002, providing modifications that modernize Federal security practices to address security concerns associated with the evolving threat landscape. These changes require less overall reporting, highlight the need for continuous monitoring, authorize the Department of Homeland Security (DHS) to implement information security policies, and direct agencies to submit annual reports including risk assessments and remediation actions.

FISMA still requires federal agencies to develop and implement agency-wide programs to secure not only their own information systems, but also those of other agencies, contractors, and third-parties with access to their networks. Coupled with prior legislation and complementary OMB and NIST guidelines, FISMA requires program officials and agency heads to implement information security programs with the goal of keeping risk at or below specified levels. The NIST Risk Management Framework supports this effort by outlining a six-step process for assessing risk and implementing security controls associated with risk magnitude.



NIST Special Publication (SP) 800-53, the industry standard for compliance, provides the recommended security controls for federal information systems and organizations and serves as

a key component of FISMA compliance. With over a hundred distinct controls, however, completely satisfying SP 800-53 is a challenge for even the most adept organization.

Of the main Security Control Families contained within NIST SP 800-53 (captured in the below table), a proper identity governance platform will address those highlighted:

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

These requirements assume a level of understanding among agency officials of the risks surrounding their organization and the security controls in place to protect their information systems. IAM solutions rooted in governance deliver this needed transparency. Given that the majority of business risk related to user access can be tied to a very small percentage of the user population, compliance with NIST SP 800-53, and by extension, with FISMA, requires identifying that small percentage and focusing on it. Unlike provisioning solutions, which view identity at the account level, governance solutions look at entitlements, giving organizations the ability to quantitatively assess which users and applications represent the greatest threat for noncompliance in a particular organization. This type of risk-based approach also gives organizations the ability to measure their risk over time and demonstrate that controls are working and reducing compliance exposure. FIDO solutions can alternately be deployed via a standalone “security key” token that contains a chip similar to the secure hardware embedded in devices. With the security key architecture, a user can use a single token across several different devices and online services, leveraging common interfaces such as USB, NFC and Bluetooth.

FICAM

In addition to playing a critical role in FISMA compliance, Identity Governance is essential to addressing Federal Identity, Credential, and Access Management (FICAM) requirements. FICAM is the set of security practices that allows organizations to administer user access privileges to the right individuals, for the right resources, and at the right times. FICAM comprises the programs, processes, technologies, and personnel needed to create trusted digital identity

representations, tie those identities to credentials, and leverage those credentials to grant access to protected physical and information resources.

The elements of FICAM compliance—identity management, credential management, and access management—are best achieved through the use of identity governance platforms that establish processes for assigning attributes to a digital identity, connecting that identity to an individual, and monitoring the data tied to that identity over its lifecycle. Traditional provisioning solutions cover only the first piece of this equation.

Legacy provisioning tools fail to understand the security models within the systems for which they provision changes. Rather than focusing on building an overall control model that understands entitlement, legacy provisioning systems focus on defining account schemas and building complex rules to control the assignment of entitlements to identities via that schema. Provisioning solutions take a "bottom up" approach to identity management—obscuring the true business policies the system executes with complex programmatic language.

By comparison, governance platforms take a "top-down" approach to ICAM by focusing on managing entitlements within a defined governance lifecycle. Governance solutions unify requests, controls, and provisioning into a single business process and facilitate FICAM compliance by building upon business-oriented assignment policies that describe who should have access to what, what data can be accessed, and what files can be shared. Together, this data creates a core governance model that describes, in business terms, how access is defined, requested, approved, tracked, audited, and reviewed.

CDM CAN HELP AGENCIES JUMPSTART IDENTITY GOVERNANCE

The Continuous Diagnostic and Mitigation (CDM) program run by the U.S. Department of Homeland Security (DHS) is playing an important role in helping agencies implement comprehensive identity governance solutions.

Phase II of the CDM program is heavily focused on raising the baseline IAM capabilities of all Federal agencies in order to continuously identify networked devices and systems, monitor users' statuses, and mitigate identified risk. Phase II requirements include:

Cred – Manage credentials and authentication

Priv – Manage account access and privilege

Trust – Manage trust for those granted access

Behave – Manage security-related behavior

Of these four components, CRED has a particular focus on identity governance, and is delivering capabilities to agencies that will serve as the cornerstone of a "Five A's" approach. CRED is focused on managing credentials and authentication. At its core, that means establishing a "master user record" governing what data and applications all employees and contractors are able to access—and then using that record to ensure they only have access to applications and resources based on their unique identity, role, and responsibility within their organization. With this record, the benefits of strong, multi-factor authentication—enabled by the PIV card—can more easily be extended to a wider array of agency applications. Additionally, agencies have the ability to more easily manage and update access privileges as roles change.

Moreover, the CRED solution identifies if and when agency authentication, reissuance, and revocation policies are incurring more risk than acceptable. This management ensures that authorized users can be authenticated appropriately for access to facilities, systems, and information.

Note that provisioning is part of the CRED solution—the automated provisioning it provides is key to securing and automatically altering privileges throughout employee lifecycles. However, it is just one feature of the broader identity governance solution.

With CRED, the CDM program will deliver some important capabilities to Federal agencies to help improve identity governance. The PRIV component of CDM is also closely tied to governance. PRIV ensures that access privileges are assigned only to authorized people or accounts that require that access to perform authorized job responsibilities. Similar to entitlement creep, granting too much access to users at the administrator and/or system level unnecessarily increases risk to an agency. Enforcing a least-privilege model, wherein employees have the minimum amount of access to applications and information necessary to perform their job function, curtails this issue. Moreover, for accounts requiring "privileged access," such as those for system administrators or other "super-users," governance solutions are essential to managing access systems tailored for privileged users and ensuring that the governance of these systems is not siloed apart from the broader IAM system.

A great benefit of the CDM program is that DHS and GSA craftily negotiated the award of the CRED solution—choosing a solution that does not just "check the box" on meeting the CRED requirements, but also gives agencies the option of applying some "bonus" features.

Simply put, government structured the license agreements with best-in-class IAM software providers to include a broad set of capabilities, while only paying for the elements required for CRED. Agencies thus have a great opportunity here to leverage the tools provided by CDM CRED to not just achieve compliance, but also drive new efficiencies in the ways their organizations work. This structuring is important, as components will need to be integrated and additional functionality will be needed beyond what CDM covers to deliver a full lifecycle approach to IAM rooted in strong identity governance.

Congress has already put ample funding behind the CDM CRED solution, covering the costs for all civilian agencies to deploy it. Agency executives should now look to take advantage of that funding, both to upgrade their IAM systems beyond outdated provisioning systems and embrace modern identity governance solutions that guard against the full range of identity-enabled cyber-attacks and enable new efficiencies in the way they do business.

CONCLUSION

While the Commission's goal of eliminating identity-enabled cyber breaches by 2021 is lofty, it is not impossible. On the contrary, by prioritizing identity governance through the lens of the Five A's, agencies can achieve both compliance and security.

ABOUT THE CHERTOFF GROUP

The Chertoff Group is a premier global advisory firm focused on security and risk management. Founded in 2009, The Chertoff Group helps clients grow and secure their enterprise through business strategy, mergers and acquisitions, and risk management security services.

With a particular focus around security and technology, The Chertoff Group provides a broad array of professional services to help our clients at every stage of the business lifecycle. We leverage our deep subject matter knowledge around important policy matters and security operations to build and execute effective strategies that enable companies to capture new opportunities and create lasting competitive advantage. For those organizations that require tactical security support, we work hand-in-hand with clients to better understand today's threats and assess, mitigate and monitor potential dangers and evolving risks in order to create more secure environments for their business operations.

Headquartered in Washington D.C., The Chertoff Group maintains offices in Houston, London, Menlo Park, and New York City. For more information about The Chertoff Group, visit www.chertoffgroup.com.

ABOUT SAILPOINT

SailPoint, the leader in enterprise identity management, brings the Power of Identity to customers around the world. SailPoint's open identity platform gives organizations the power to enter new markets, scale their workforces, embrace new technologies, innovate faster and compete on a global basis. As both an industry pioneer and market leader in identity governance, SailPoint delivers security, operational efficiency and compliance to enterprises with complex IT environments. SailPoint's customers are among the world's largest companies in virtually every industry, including: 9 of the top banks, 7 of the top retail brands, 6 of the top healthcare providers, 6 of the top property and casualty insurance providers, and 6 of the top pharmaceutical companies.

SailPoint: The Power of Identity™