SailPoint

WHITE PAPER

Identity Governance and **Compliance for Federal Agencies**

Cyber attacks on government networks are becoming increasingly sophisticated, frequent and dynamic. Adversaries take advantage of outdated or inadequate cybersecurity solutions and use them as the vector of attack. Insider threats and external attacks continue to be a top priority for federal agencies that must comply with a number of cybersecurity standards. The need for identity governance solutions to guard against the full range of identity-centered cyber attacks, and to enable new efficiencies in the way our government conducts business, has never been greater.

> Most of the recent cyber attacks have been a result of poor identity management and controls. Many agencies still have traditional identity and access management solutions that only provide limited automated management, provisioning and basic reporting capabilities, and they rely heavily on significant human interaction.

The Department of Homeland Security has made a significant investment for each federal agency to report the accuracy of the Master User Record (MUR) for employees and contractors on the agency network. Agencies have the ability to enhance the Continuous Diagnostics and Mitigation (CDM) solution from SailPoint to improve the efficiencies and accuracy of Federal Information Security Management Act (FISMA) reporting, while increasing their cybersecurity posture. Additional product functionality is available from SailPoint to extend agencies' current Federal Identity Credential and Access Management (FICAM) environment and achieve complete governance over privileged and non-privileged users, access to entitlements, applications and resources.

For CDM Phase 2, the Department of Homeland Security selected SailPoint's IdentityIQ Unified Governance Platform and Compliance Manager to manage attributes for identities and security controls in four functional areas – TRUST, CRED, BEHAVE and PRIV – to create a MUR for privileged and non-privileged users on the agency network. Each agency may leverage the DHS investment and take full advantage of the licensed implementation of the platform and can extend the capabilities with additional SailPoint product offerings.

This document suggests opportunities and guidance based on the SailPoint platform to accomplish FICAM objectives.

CDM Phase 2 Solution Overview

The Department of Homeland Security CDM Project Management Office and the System Integrators for the PRIVMGMT, CREDMGMT and TO2F Task Orders collaboratively developed the solution for the MUR, which is a set of attributes or assertions about a user that will be integrated with the government-wide CDM Dashboard for Enterprise Risk Assessment, in accordance with a predetermined set of CDM metrics. The functionality of the MUR solution encompasses the following:

- Connection to agencies, authoritative sources
- Correlation of privileged and non-privileged users identities and accounts
- Identification of users status and suitability for access to agency networks and entitlements
- Provide visibility in consolidated reports and metrics for agency evaluation.

Where Do Agencies Go from Here?

While the CDM solution may integrate with an agency's Identity, Credential and Access Management (ICAM) systems, the CDM MUR solution was not intended by the Department of Homeland Security to provide FICAM capabilities to the agency. Rather, the MUR provides agencies with a baseline understanding of who is on the network and what privileged accounts they can access. The capability to actively assign roles, enforce segregation of duties, access policies, and access requests, approvals and certifications is not included in the delivered solution.

Agencies can fully accomplish FICAM services architecture goals, increase cybersecurity posture, and reduce overhead and complexity in identity management activities, auditing and FISMA reporting by taking full advantage of the SailPoint offerings and technologies.

The Federal Identity Crisis

The management of identities, entitlements and privileges continues to be among the top concerns of federal cyber initiatives. Identity-related activities are needed to protect sensitive information and resources across the federal government, as defined by the FISMA and the Office of Management and Budget Memos 16-04 ("Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government"), 15-01 ("Guidance on Improving Federal Information Security and Privacy Management Practices)" and 14-03 ("Enhancing the Security of Federal Information and Information Systems").

Access controls have been widely enforced on most agency systems with the PIV-card, but have limited integration with full-lifecycle entitlement management and governance process that results in orphaned accounts, excessive rights and overexposed sensitive data. The systems do not provide a deep understanding of identities, entitlements, behavior or compliance. As a result, some agencies continue to struggle with FISMA auditing and cyber-forensics due to the lack of a modern identity governance solution.

> Many agencies still have traditional identity and access management solutions that only provide limited automated management, provisioning and basic reporting capabilities, and they rely heavily on significant human interaction and analysis that results in high productivity costs for administrators and analysts.

The CDM MUR and FICAM

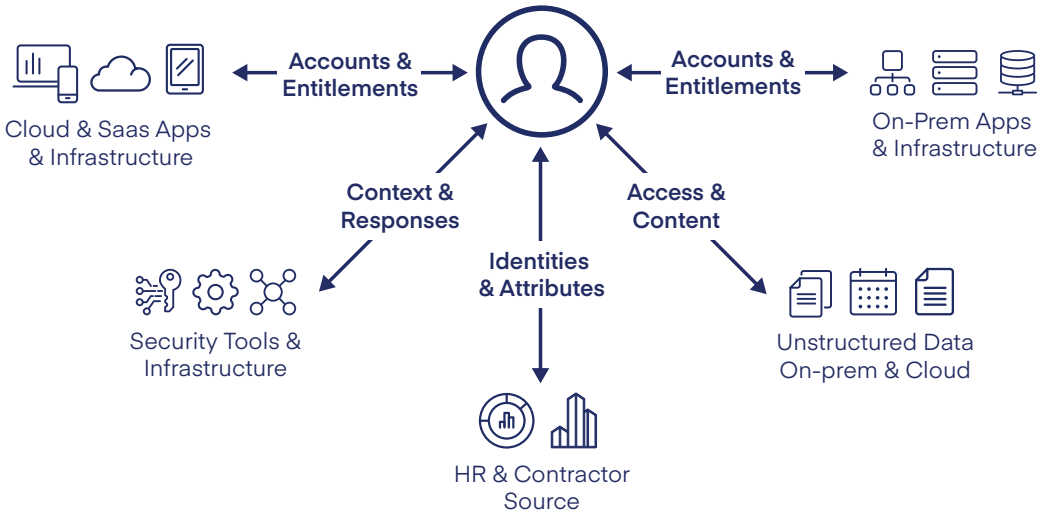
The four capability areas of the CDM MUR are closely related to the U.S. General Services Administration's FICAM program and create a centralized identity record that will be the primary key for CDM dashboard reporting and FISMA metrics. FICAM comprises the many processes and technologies for establishing and maintaining identity and credentials to automate and enable access to networks, applications and physical assets. Each area works cohesively with related services to provide agencies with robust capabilities to prevent, detect and mitigate many of the threats associated with access lifecycle management. FICAM services are key enablers for generating data for agencies to mitigate threats and monitor.

The SailPoint solution implements the capabilities of the FICAM services architecture and extends identity governance capability with access certifications, risk profiles, data access governance and advanced analytics.

Identity Management	**FICAM Activity:** Creation, Maintenance, Identity Resolution, Deactivation **FICAM Keywords:** Identity Lifecycle Management, Identity Record, Authoritative Source, Updating, Attribute Management, Account Linking, Suspension, Archiving, Deletion **SailPoint Capability:** Identity Warehouse, Connector and Integration Framework, Identity Aggregation, Identity Correlation, Unified Governance Platform, Lifecycle Manager
Credential Management	**FICAM Activity:** Registration, Issuance, Maintenance, Revocation **FICAM Keywords:** Enrollment, Suspension, Termination **SailPoint Capability:** Identity Warehouse, Connector and Integration Framework, Unified Governance Platform, Lifecycle Manager
Access Management	**FICAM Activity:** Policy Administration, Entitlement Management, Provisioning, Authorization **FICAM Keywords:** Account Management, Privilege, Right, Access Management, Access Reconciliation, Policy Decision, Workflow **SailPoint Capability:** Identity Warehouse, Connector and Integration Framework, Unified Governance Platform, Policy Model, Role Model, Risk Model, Lifecycle Manager, Compliance Manager, Access Certification
Federation	**FICAM Activity:** Attribute Exchange **FICAM Keywords:** Attribute Definition **SailPoint Capability:** Identity Warehouse, Connector and Integration Framework, Unified Governance Platform, Policy Model, Role Model, Risk Model, Lifecycle Manager
Governance	**FICAM Activity:** Audit & Reporting, Redress, Recovery **FICAM Keywords:** Data collection, Monitoring, Analysis, Data certification, Remediation, Mitigation **SailPoint Capability:** Unified Governance Platform, Policy Model, Role Model, Risk Model, Compliance Manager, Access Certification, Reporting, Advanced Intelligence, Security integration, Business Process, Workflow

Accomplishing FICAM Objectives with the SailPoint Solution

For federal agencies, an identity solution should go beyond simple management and authentication, and take a governance-based approach as enterprise security has entered a new era and is evolving from being network-centric to identity-centric. Perimeters are being redefined by complex relationships between people and data, of which most traditional identity solutions have not been able to effectively address. The job of identity governance is simple in principle: give the right people the right access to the right data. To do this, trusted and properly managed identity access must become the primary control. Governing access comes down to three basic questions:



1 **Who has access today?**
This is a matter of inventory and compliance. It starts with understanding the current state, and it involves cataloging and understanding access to ensure it is correct.

2 **Who should have access?**
Models and automation are the cornerstones to determining who should have access. Before asking whether or not a specific person should have access to a file, you need to know more about who that person is and what role they have within your agency. You must then understand and classify the data they are attempting to access. Next, establish a model that defines if that person's access conforms to his pre-defined policy. While partitioning data this way may be more complex, it is critical to implementing any form of preventive controls.

3 **Who had access?**
Determining prior access is a matter of monitoring and audit. It is no longer enough to understand who has and should have access. It is vital for IT security forensics and auditing to identify who was actually granted access, in addition to when and what endpoint was last used.

Building from the agency's centralized MUR, agencies can extend the capabilities of the SailPoint platform and implement a FICAM solution rooted in governance. SailPoint IdentityIQ is a modern identity governance solution comprised of a base unified governance platform, lifecycle manager, compliance manager and a privileged access management integration module. SecurityIQ extends identity governance to data stored in files across on-premises and cloud repositories. Furthermore, IdentityIQ and SecurityIQ are complete with a flexible connectivity model and integrated interface that simplifies the management of applications and data in the datacenter or the cloud.

Open Identity Platform

SailPoint's open identity platform lays the foundation for effective and scalable identity governance within an agency. It establishes a common framework that centralizes identity data, captures business policy, models roles and takes a risk-based, proactive approach to managing users and resources.

The open identity platform is fully extensible, providing:

- Robust analytics that reconciles and transforms disparate and technical identity data into relevant business information
- Resource connectivity that allows organizations to directly connect IdentityIQ to applications running in the datacenter or in the cloud
- APIs and a plugin framework for customers and partners to extend IdentityIQ to meet a wide array of needs

The platform allows organizations to build a single preventive and detective control model that supports all identity business processes, across all applications. SailPoint IdentityIQ applies consistent governance across compliance, provisioning and access management processes – maximizing investment and eliminating the need to buy and integrate multiple products.

Lifecycle Management

IdentityIQ Lifecycle Manager manages changes to entitlements and access through user-friendly self-service request, password management interfaces and automated lifecycle events. It provides a flexible, scalable provisioning solution for addressing the constantly evolving access needs of your business in a way that's both efficient and compliant.

The importance of attribute currency in decision making

SailPoint's extensive connectors and integration modules provide links into applications, repositories and cloud services to create the complete view of an identity. Attributes about a user, such as the status or level of a security clearance, training or industry certification, credential, job title or location, may be used in

automated provisioning, granting access to entitlements, privileges or data. Thus, the information must be current and accurate. The MUR provides agencies with a solid baseline to make timely decisions to ensure the right people are granted access to the right data.

Agencies can extend the deployment of the MUR to include additional attributes and data about identities. Attributes can be used to create "populations" of users for assignment and analysis, make dynamic decisions for role, entitlement and privileges, calculate application and user risk scores, and enrich detailed reports and metrics.

Business Role and Entitlement Management

SailPoint's Role Modeler allows agencies to implement an enterprise role model to simplify compliance and provisioning processes for users. It helps enterprises align low-level IT privileges with their structure and operations by grouping individual entitlements into higher-level business functions. It further abstracts users from the underlying complexity of IT authorization models. IdentityIQ roles are designed to be highly flexible and customizable. This flexibility allows IT to model a wide array of structures and IT functions without the need for custom coding. The Role Modeler enables organizations to create roles that enforce "least privilege" access while helping to control role proliferation, a common challenge within role projects. IdentityIQ's role mining functionality speeds and simplifies the creation of roles that accurately represent the organization's business and IT needs, and its role lifecycle management capabilities help organizations keep the role model up to date with changes in the business and IT structures.

The privileged accounts and systems aggregated by the MUR can be modeled into roles that can then be dynamically or directly provisioned and deprovisioned. Policies can be configured to ensure segregation of duties on roles to ensure data privacy and adhere to access and compliance controls.

Self-Service Access Request

IdentityIQ creates an entitlement catalog from managed systems entitlements. The entitlements and roles are available to users in the business-friendly, self-service interface, which provides the ability to search, request and model access requests. Access requests can be made by an individual, supervisor, application owner or administrator. The request process initiates a business-process workflow to begin the provisioning steps. The process performs a policy evaluation before it begins the approval process to ensure adherence to access and compliance policies.

Governance & Compliance

IdentityIQ Compliance Manager automates access certifications, policy management and audit reporting through a unified governance framework. This enables agencies to streamline compliance processes and improve the effectiveness of identity governance.

Enterprise Access and Policies

Enforcing access policies is a critical component of any compliance solution. SailPoint enables agencies to define policies in areas such as entitlements and segregation of duty, and then automatically scans for violations across on-premises and cloud-based resources. SailPoint also allows organizations to:

- Enforce multiple types of policies across applications and other resources
- Identify violations proactively so they can be addressed before they create major problems
- Mitigate violations in real time

Configured policies in SailPoint may use the MUR attributes to further enforce enterprise access controls and cyber defense, and to define and enforce compliance controls and risk.

For example, a policy may be configured to assess the MUR to ensure someone with the role/job title of system administrator, who is also a member of the System Administrators group in Active Directory, has completed cybersecurity awareness training. The configuration would further ensure that the individual has signed the system rules of behavior, possesses a current CISSP certification, is in the Information Technology department, or is an active user in Active Directory and the Personnel Management System. If the evaluation of the policy fails, IT administrators, business owners and data stewards can take various actions such as Access Remediation, Account Suspension/Removal, Notification/Alerting and Reporting can be taken.

Validating that a user's access privileges align with their role within an organization is essential to complying with FISMA regulations and ensuring information integrity and privacy.

Access Certifications

SailPoint automates the process of regularly validating user access privileges to reduce the chances of noncompliance and improve overall risk posture. SailPoint's compliance solution drives automated review cycles, and presents data in language and terms that are accessible to both IT and business users. It further supports periodic, event-triggered and continuous certification options.

Access Certifications can be configured for application access and assigned to business owners or supervisors, removing the burden from the IT department and placing responsibility on those closest to the application or data. Access Certifications in IdentityIQ can reduce the time to complete a review process from weeks and months to mere days. This increases an agency's ability to comply with FISMA regulations more quickly and accurately than ever before, while ensuring a least privilege posture is being enforced across all agency systems and data.

Risk-based Access Controls

IdentityIQ Lifecycle Manager manages changes to entitlements and access through user-friendly self-service request, password management interfaces and automated lifecycle events. It provides a flexible, scalable provisioning solution for addressing the constantly evolving access needs of your business in a way that's both efficient and compliant.

Finally, with a risk-based approach, agencies can measure their risk over time to demonstrate controls are working and reducing compliance exposure.

Considering the earlier example, a risk value may be assigned to the policy violation for missing a particular training or certification. That risk value may be higher or lower, depending on the role or access. A cumulative risk score may be used to identify riskier users and applications, and further monitor their behavior or remove access privileges. Risk values can also be used in processes for determining the approval path for additional entitlements.

Metrics, Analytics and Reporting

SailPoint offers extensive tools for improving decision making and audit performance, including risk analytics, intuitive interfaces for gathering intelligence, business context to make technical information more accessible to business users, and complete transparency to user access. The information business users need to have to determine the necessary steps for protecting the agency's compliance status is always instantly available and easy to apply to the decision-making process.

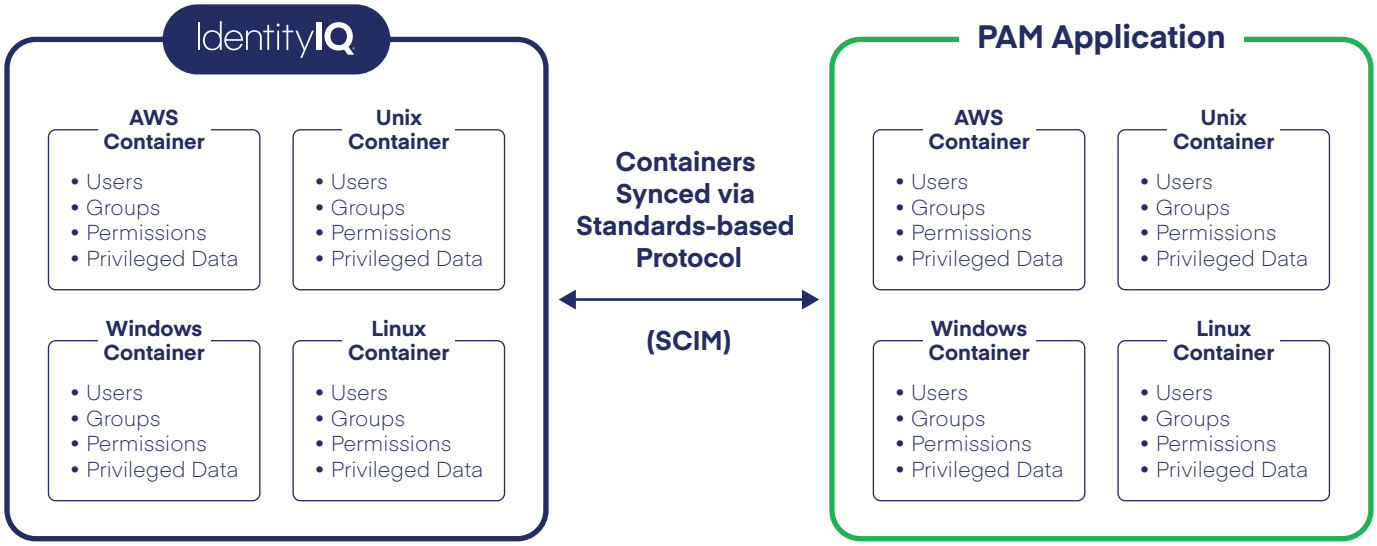
SailPoint leverages identity intelligence to transform technical identity data scattered across multiple enterprise systems into centralized, easily-understood and business-relevant information. SailPoint serves up compliance information in a variety of flexible formats, including dashboards, reports and advanced analytics, that can be used by compliance administrators, auditors and business management.

As demonstrated in the limited reports provided by the MUR solution, agencies can take full advantage of the identity intelligence platform to reduce the complexity and overhead of FISMA reporting.

Privileged Account Management

Privileged users and entitlements for a subset of systems are part of the MUR solution. The integration provided by the PRIVMGMT solution does not fully integrate the agency's PUM solution with SailPoint. SailPoint has extensive relationships with the leading PUM vendors and has developed solutions based on the open-identity platform, connectors, plug-in framework and Secure Cross-domain Identity Management.

SailPoint IdentityIQ Privileged Account Management (PAM) Module extends identity governance processes and controls to highly-privileged access, enabling agencies to centrally manage access to privileged and non-privileged accounts.



The SailPoint IdentityIQ Privileged Account Management Module enables agencies to:

- Establish complete visibility and governance across all privileged accounts
- Automate governance controls, providing a complete view of an identity's access and its associated privileged accounts, eliminating over-entitled users
- Gain visibility to all user access, including privileged accounts
- Aggregate container/safe contents beyond accounts
- Search and filter, allowing admins to quickly query who has access
- Eliminate waiting for privileged access by synchronizing lifecycle events
- Mitigate entitlement creep and orphaned privileged accounts via timely provisioning
- Reduce error-prone fulfillment with automated provisioning
- Consolidate certifications for privileged and non-privileged accounts
- Certify users have the right access to the right safes
- Extend IdentityIQ separation of duty policies to include privileged access
- Speed the delivery of provisioning and deprovisioning privileged access based on lifecycle event changes
- Rapidly deploy and integrate with your PAM vendor of choice, through a model using a standards–based integration framework

Integration with third party PAM solutions

The IdentityIQ Privileged Account Management Module enables agencies to deploy and integrate with the PAM vendor of choice. The IdentityIQ Privileged Account Management Module provides an open, standards–based integration framework that supports any third-party Privilege Account Management solution.

Extending Identity Governance to Data Stored in Files

Managing access to data stored in files (.docx, .ppt, .xls, .pdf, .csv, .txt, etc.) is a growing problem for agencies. The amount of data stored in file servers, network attached storage devices, collaboration portals such as SharePoint, Exchange mailboxes and cloud storage systems (DropBox, Box, OneDrive, Google Drive, etc.) has increased exponentially over the past few years and is projected to grow 800% in the next five years.

By governing access to sensitive data, SecurityIQ extends the SailPoint identity governance platform to provide a comprehensive approach across all applications and files. SecurityIQ delivers enterprise-level identity governance by discovering where sensitive data resides and applying appropriate access controls. It also provides real-time visibility to improve security, mitigate compliance risks and support greater efficiency across on-premises or cloud storage systems.

SecurityIQ helps agencies meet regulatory requirements by providing proof of compliance during audits and increases staff productivity by reducing time spent on diagnostics, forensics and data administration tasks. It also simplifies the ongoing challenge of managing how users are granted access to sensitive files and folders throughout a user's lifecycle within the organization.

Identify and Classify Sensitive Data

Agencies with unmanaged, unprotected files face significant risk. And given the sheer volume of data files within many organizations, securing this data may appear overwhelming. SecurityIQ reduces risk by cutting through the clutter to discover and classify sensitive data.

- Identify where sensitive data resides on-premises or in the cloud using keywords, wildcards and regular expressions
- Utilize content and behavior-based approaches to classify sensitive data
- Model who has access to what data and how it is granted
- Monitor who is accessing data in real-time, and maintain visibility with actionable dashboards

Establish Data Ownership

Across many organizations, there is not an established framework for the ownership of data stored in files. As business users create the majority of this type of information, they often have the most knowledge about this data and who should have access. SecurityIQ provides an automated process that leverages crowd-sourcing to accurately allow the users most active with the data to nominate the true data owner. With SecurityIQ, you can:

- Monitor files for activity by user and report on user access behavior patterns
- Determine which users or departments are accessing the data most often
- Utilize a crowd-sourced survey to enable the business to vote on the most relevant data owner
- Leverage survey results to appoint the best data owner as the primary custodian

Mitigate Security Risks

Securing access to data stored in files is impossible to manage and control without full visibility and control of data. SecurityIQ automatically collects and analyzes effective permissions across on-premises Windows file-servers, network attached storage devices, SharePoint and Exchange, as well as cloud-based portals, including Office 365, Box, Dropbox and Google Drive. To prevent security breaches and information theft, or minimize the potential damage of this activity, agencies need real-time monitoring of users that access sensitive files or change file permissions, as well as the ability to respond to violations. SecurityIQ enables organizations to:

- Address permissions creep and establish one permission path per user with access normalization and cleanup
- Identify and remediate overexposed access to sensitive data (file shares, SharePoint, DropBox, etc.)
- Monitor for cybersecurity threats and respond to policy violations with real-time alerts
- Identify the root cause of and utilize forensic analysis to trace the threat origin

Address Compliance and Audit Requirements

In the face of proliferating regulations, organizations continue to face a variety of compliance hurdles, including the inability to identify sensitive information, difficulty responding to audits, and maintaining adequate control around data access. SecurityIQ can help agencies accelerate compliance readiness by:

- Creating and enforcing access policies and only granting access on a "need-to-know" basis
- Discovering and classifying PII with out-of-the-box policies
- Streamlining audit processes with automated access reviews and certifications
- Demonstrating proof of compliance with real-time reports across all data access

Summary

The Department of Homeland Security has made a significant investment for each agency to aggregate, correlate and report the accuracy of the data elements in the MUR. Agencies have the ability to enhance the CDM SailPoint solution to the efficiencies and accuracy of FISMA reporting, while increasing each agency's cybersecurity posture. Additional product functionality is available from SailPoint to extend an agency's current FICAM environment and achieve complete governance over privileged and non-privileged users, and access to entitlements, applications and resources.

SAILPOINT: THE POWER OF IDENTITY™

sailpoint.com

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 a wide range of industries, including: 6 of the top 15 banks, 4 of the top 6 healthcare insurance and managed care providers, 8 of the top 15 property and casualty insurance providers, 5 of the top 15 pharmaceutical companies, and six of the largest 15 federal agencies.

WP1192-1801