U.S. DEPARTMENT OF THE INTERIOR
MARCH 3, 1849

United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, DC 20240

DEC 0 1 2015

Memorandum

To: Heads of Bureaus and Offices
Assistant Directors for Information Resources

From: Sylvia Burns
Chief Information Officer Sylvia Burns

Debra Sonderman Debra E. Sonderman
Director, Office of Acquisition and Property Management
Senior Procurement Executive

Subject: Mandatory use of Security Assertion Markup Language (SAML) 2.0 Standard for Cloud-Based, Web Application Authentication Information Exchange

The Department of the Interior's (DOI) Cloud Strategy is focused on enabling our employees with powerful web technologies that enable them to effectively deliver the mission and transform and modernize the organization's data sharing capabilities – with internal and external partners and the American people. DOI's Foundation Cloud Hosting Services Contract (FCHC), awarded in 2013, is the primary avenue for obtaining cloud services.

The diversity of DOI's mission, its geographic distribution, often in very remote locations, and the resultant distribution of its workforce define the organization and drive real technology and connectivity challenges that ubiquitous cloud services can address. As more and more web systems and services migrate to the cloud, DOI employees face the potential proliferation of independent userIDs and passwords, many of which may not meet Federal Personal Identity Verification (PIV) standards. Secure and effective use of the cloud requires a standard for authentication to cloud-based web services using authoritative DOI PIV credentials.

The Security Assertion Markup Language (SAML) provides an open, interoperable, XML-based framework for exchanging user authentication, entitlement, and attribute information between providers of web services (cloud providers) and the holder of credentialing information (DOI). SAML permits DOI to make assertions regarding the identity, attributes, and entitlements of a user account to an external web service.[1]

[1] See https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

Adoption of the SAML standard for the exchange of authentication information is central to the agency's successful implementation of the Federal Identity, Credential, and Access Management (FICAM) strategy and corresponding two-factor PIV authentication requirements for cloud-based web applications and services. The standard allows the Department to meet its requirement to accept credentials issued by trusted external parties when authenticating to the agency's Levels of Assurance (LOA) 1 and 2 web systems as identified in the Federal Chief Information Officer Memorandum, "Requirements for Accepting Externally-Issued Credentials."[2]

The SAML standard also provides clear and repeatable guidance for the interoperable exchange of authentication information that DOI's FCHC providers require in order to consistently respond to web-oriented task orders. Requiring SAML as an authentication standard removes a burden on cloud providers, reduces the proliferation of externally managed, additional employee logon IDs and passwords for web systems and services, and eliminates the potential exposure of credential information at cloud-based providers' systems.

Effective immediately, all DOI purchases or implementations of cloud-based web services and systems that require logon by DOI employees at large must support DOI's SAML 2.0 standard and must be configured to authenticate using DOI's Identity Provider prior to entering production. The sole DOI Identity Provider is operated by OCIO's Service Delivery Division as a shared service for the benefit of all of DOI and is the Department's only approved SAML solution. This shared service must be used for all DOI cloud-based web services that require DOI user authentication.

This policy memorandum supplements the January 6, 2014, memorandum "*Mandatory Use Policy for DOI Foundation Cloud Hosting Services Contracts*" and applies to the procurement of all Cloud-based Web services through this or any other vehicle.

If you have questions of a technical nature, please contact steven_argo@ios.doi.gov. To obtain the proper language for insertion in a new solicitation, please contact Cloud@ios.doi.gov

cc: Deputy Assistant Secretary – Technology, Information, and Business Services
Deputy Assistant Secretary - Budget, Finance, Performance, and Acquisition
Bureau Chief Financial Officers
Office of the Chief Information Officer Executive Staff
Bureau Procurement Chiefs
Charge Card Agency/Organization Program Coordinators
Charge Card Bureau Leads
Director, Office of Small and Disadvantaged Business Utilization

[2] http://www.cio.gov/Documents/OMBReqforAcceptingExternally_IssuedIdCred10-6-2011.pdf