Department of Justice (DOJ) Fiscal Year 2024 Agency Report

1. Please provide a summary of your agency's activities undertaken to carry out the provisions of OMB Circular A-119, "Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities" and the National Technology Transfer and Advance Act (NTTAA). The summary should contain a link to the agency's standards-specific website(s) where information about your agency's standards and conformity assessment related activities are available.

Led by the Attorney General, the Department of Justice (DOJ) is comprised of more than 40 separate component organizations and has approximately 115,000 employees who carry out the missions of the Department. While the DOJ's headquarters are in Washington, D.C., it conducts most of its work in field locations throughout the country and overseas. The mission of the Department of Justice is to uphold the rule of law, to keep our country safe, and to protect civil rights.

DOJ uses standards wherever reasonable, recognizing the importance of Voluntary Consensus Standards (VCS) in achieving its mission goals. Implementation of VCS in both Departmental systems and those funded by Departmental grants:

- Improves collaboration and cooperation with criminal justice partners and the private sector;
- Makes services, products, and systems development more efficient (including cost and/or implementation time savings);
- Ensures equipment and systems are of the highest quality, safe, and effective as well as compatible and interoperable;
- Supports innovation, free and fair competition, commerce or trade while avoiding duplication of private sector activities;
- Ensures the results of analysis are unbiased and scientifically valid;
- Provides validation that facilities are operating safely, effectively, and are managed in accordance with sound principles;
- Enables reuse of technical tools to support multiple projects, reduce dependency on custom solutions; minimize project risk, and reduce dependency on a too specialized workforce;
- Provides an opportunity to pull communities-of-interest together;
- Allows commercial industry to reduce product development costs and pass those cost savings on to the Department;
- Improves procurements, contracting, and grant making functions.

The following summarizes some of DOJ's standards and conformity assessment activities in 2024, demonstrating the Department's active participation in improving and applying standards to deliver the mission.

Initiatives at the Department level include:

- **Deputy Attorney General's eLitigation Modernization Effort:** This cross-component commission supported work to assess the development and use of consensus standards across litigation activities to support modernization, compliance and workforce development efforts. These efforts are based in part of federal statutes and authorities, industry standards and Department policies and practices.

- **Emergency Technology Board (ETB):** Chaired by the Department's Chief Artificial Intelligence Officer (CAIO), the ETB was established pursuant to Office of Management and Budget directive and Department policy, and is tasked with developing policy and regulations in connection with DOJ procurement and use of technologies containing Artificial Intelligence (AI) capabilities, and

other emerging technologies. The ETB is currently working on implementing the provisions of M-25-21, *Accelerating Federal Use of AI through Innovation, Governance, and Public Trust* and M-25-22, *Driving Efficient Acquisition of Artificial Intelligence in Government*.

- **DOJ Facial Recognition Technology Working Group (FRT WG):** This Working Group was charged with identifying operational and administrative uses of FRT across the Department and developing standards for such use in line with National Institute of Standards & Technology accepted principles, industry best practices, and federal law. The FRT WG produced a DOJ Interim Policy on the use of FRT. This policy underwent subsequent discussion and revision in FY2024.

- **DOJ Data Brokers Working Group (DBWG):** This Working Group was tasked with evaluating the Department's procurement and use of commercially available information (CAI) and ensuring CAI is lawfully obtained with oversight, accountability, equity, and transparency. The Working Group contributed substantially to the creation of Department policy governing the acquisition and use of commercially available information.

The Department's Office of the Chief Information Officer leads several efforts in support of the development and use of Voluntary Consensus Standards and Conformity Assessment Activities, including:

- **ISO 20000-1 (Service management) and 27001 (Information Security) Standards:** The Department actively applied both standards in our delivery of IT and information security services including formal external certification body audits to maintain ongoing ISO certification. The original certifications were obtained in 2015, and upgraded to ISO 20000-1:2018, and ISO 27001:2022. Although our certifications have been forfeited due to budgetary impacts in April 2025, we maintain operational activities and remain ISO compliant. Application of these standards ensures the continuous evaluation of service performance and use of standard practices as defined by criteria well-recognized across industry and government.

- **Data Governance Board (DGB)**: Chaired by the Chief Data Officer, the DGB addresses DOJ data management standards, priorities, policies, and practices. The Board serves as the leader for coordinating and facilitating implementation of Department-wide processes and standards, and for addressing common issues affecting Component data programs and resources. The DGB includes members from the following Components: Bureau of Alcohol, Tobacco, Fires and Explosives (ATF), Federal Bureau of Prisons, Civil Division, Criminal Division, Civil Rights Division, Drug Enforcement Administration (DEA), Environment and Natural Resources Division, Executive Office for Immigration Review, Executive Office for United States Attorneys, Federal Bureau of Investigation (FBI), Justice Management Division (JMD), Office of Inspector General, OJP, and United States Marshals Service (USMS). The DOJ Data Governance working groups that encourage participation from Components are as follows:
    - **Data Architecture Working Group (DAWG):** Developed consistent data governance standards within the DOJ across several key areas. This includes in the procurement and use of Commercially Available Information (CAI), data lexicons, Data Management plans, and other areas of alignment. These standards and assessment relate to the DOJ Data Governance Board oversight efforts and incorporate industry data standards, federal statutes and other authorities.
    - **DOJ Geospatial Community of Interest (GCOI)**: Chaired by DEA, FBI, and JMD, the GCOI met quarterly and continued raising awareness on critical geospatial topics and activities pertaining to standards. The GCOI provided oversight for implementing geospatial standards and continued progress in meeting the Geospatial Data Act requirements, including the distribution of job-aids that refer to open international

standards, metadata standards implementation, and standards development to support enhanced interoperability and equitable access to all DOJ geospatial data users.
    - **Artificial Intelligence Community of Interest (AI COI):** Unites DOJ employees who are interested in accelerating the thoughtful adoption of AI, the coordination of AI initiatives, the implementation of Department-wide AI processes and standards, and the discussion of common AI issues or concerns among Components.
    - **Identity, Credential, and Access Management (ICAM) Working Group:** Focused on the Identity, Credential and Access Management capabilities of the Department's Data Strategy.

- **DOJ Internet of Things (IoT) Working Group**: Aligns cross component compliance with IoT Act of 2020 and OMB M-25-04 requirements and NIST standards. Gather critical insights and information on the challenges of compliance, identify opportunities, best-practices, and solutions to support compliance, and move the department forward toward securing IoT assets within the enterprise.

The FBI has not identified the need for any government unique standards in lieu of consensus-based standards. The FBI's Field Services Response Branch (FSRB) ensures the FBI is represented in appropriate Standards Development Organizations (SDOs) and bodies to position the FBI to develop and exploit technology in ways that recognize and protect civil liberties, allows for auditing of use, and enables the FBI mission. The FBI's centralized SDO authority resides with the Internet Governance (IG) and 5G Program Office led by an FBI Senior Leader. FSRB and its corresponding divisions, including Criminal Justice Information Services Division (CJIS), Operational Technology Division (OTD) and the Laboratory Division (LD) follow the policies of OMB Circular A-119 by regularly participating with commercial and private-sector on standard development of voluntary consensus standards via committees, working groups, meetings, conferences, and other engagements. The FBI's FSRB regularly participates in the following SDOs and bodies:

- **(U) International Telecommunications Union (ITU).** The FBI regularly attended ITU meetings which allocates global radio spectrum and satellite orbits, develops the technical standards that ensure networks and technologies seamlessly interconnect, and strive to improve access to ICTs to underserved communities worldwide. Standardization development and coinciding work is conducted via study groups. In FY2024, the FBI participated in two ITU study groups.

    - (U) Study Group 17 (SG-17) – This study group is responsible for initiating standards work on security, identity management, and other security aspects on ICT. In FY2024, the FBI substantially supported a contribution around Digital Identities for consensus to begin work within SG-17 in FY2025.
    - (U) Study Group 21 (SG-21) – This study group is responsible for multimedia technologies and has assumed the lead in Artificial Intelligence (AI) studies around ICTs. In FY 2024, the FBI was active in this newly aligned study group related to AI activities.

- **(U) Internet Governance Forum (IGF):** The FBI continued to be an active participant in this global forum hosted by the United Nations Department of Economic and Social Affairs (UNDESA) and administered by the Multi-stakeholder Advisory Group (MAG).

    - (U) In FY2024, the FBI's proposal to host a panel on lawful access and child online safety was accepted by the MAG. The panel occurred in FY2025 and examined the complex balance between safeguarding children online and protecting individual privacy rights

and addressed the ethical, legal, and practical challenges involved.

- **(U) National Information Exchange Model (NIEM):** Subject Matter Experts (SME) from the FBI's OTD participated in bi-weekly meetings with NIEM through FY2024 and advised on the exchange of audio and voice information. NIEM defines standard terminology, models, and relationships for the exchange of data across public and private organizations. In early FY 2025, the working group completed four-year effort to develop proposed standard terminology for submission to the International Committee for Information Technology Standards.

- **(U) The 3rd Generation Partnership Project (3GPP):** The FBI continues to participate in development of service-based interception capabilities for 5G-based communication services in 3GPP. This participation is meant to satisfy the industry consultation requirements of the Communications Assistance for Law Enforcement Act (CALEA) for the development of industry standards for covered services.

- **(U) Alliance for Telecommunications Industry Solutions (ATIS):** The FBI continues to participate regarding Packet Technology and Systems Committee (PTSC) and lawfully Authorized Electronic Surveillance (PTSC LAES). ATIS is a standards organization that develops technical and operational standards and solutions for the ICT industry.

- **(U) Internet Engineering Task Force (IETF):** IETF develops technical standards of the internet's architecture including encryption, cybersecurity, network security, routing and other key protocols. The FBI continues to satisfy the industry consultation requirements of CALEA for the development of industry lawful intercept specifications for covered services.

- **(U) European Telecommunications Standards Institute (ETSI):** The ETSI develops global technical standards for ICT- enabled systems, applications, and services. The FBI continues to participate in regard to the Technical Committee for Lawful Interception (ETSI TC-LI) to satisfy the industry consultation requirements of CALEA for the development of industry lawful intercept specifications for covered services.

- **(U) Cable Television Laboratories, Inc. (Cable-Labs):** Cable-Labs develops global technical standards for broadband internet access services. The FBI continues to participate to satisfy the industry consultation requirements of CALEA for the development of industry lawful intercept specifications for covered services.

The Office of Justice Programs' (OJP) National Institute of Justice (NIJ) fosters development of equipment standards and related conformity assessment programs that specifically address the needs of law enforcement, corrections and other criminal justice agencies. The goal is to ensure to the degree possible that equipment is safe, reliable and performs according to established minimum requirements. More about NIJ's standards and conformity assessment activities can be found at https://nij.ojp.gov/topics/equipment-and-technology/standards-and-conformity-assessment.

NIJ continues to operate its NIJ Compliance Testing Program (CTP) for law enforcement body armor. In FY 2024, 43 models of ballistic-resistant body armor were submitted to the NIJ CTP for testing at accredited commercial laboratories recognized by NIJ. In addition to initial testing, follow-up inspection and testing was conducted on 151 models complying with NIJ Standard 0101.06, *Ballistic Resistance of Body Armor.* In addition, 14 models of stab-resistant body armor were submitted to the NIJ CTP for testing in accordance with NIJ Standard 0115.00, *Stab Resistance of Personal Body Armor*. NIJ publishes its Compliant Products List for armor models that meet the program requirements at https://nij.ojp.gov/topics/equipment-and-technology/body-armor/ballistic-resistant-armor.

NIJ continues to participate in ASTM International Committee E54 on Homeland Security Applications which develops and publishes voluntary consensus standards (VCS) focused on methods and practices to test ballistic-resistant and other life safety equipment as well as standards for testing law enforcement public order personal protective equipment. In FY2024, NIJ published NIJ Standard 0101.07, *Ballistic Resistance of Body Armor*, a voluntary equipment performance standard for torso-worn body armor for law enforcement, which incorporates ten ASTM VCS, and updates the prior NIJ version. In FY2024, NIJ also published NIJ Standard 0123.00, *Specification for NIJ Ballistic Protection Levels and Associated Test Threats*, a voluntary specification that defines ballistic protection levels and associated test threats and incorporates three ASTM VCS. NIJ's body armor standard was first published in 1972 and is widely used by industry and law enforcement agencies as a benchmark for their body armor. NIJ developed these voluntary equipment performance standards using consensus methods, including gathering input from a wide range of stakeholders through workshops and public comment, using VCS published by ASTM, and using a Special Technical Committee composed of federal, state, and local law enforcement subject matter experts; ballistics laboratories; and other technical experts to establish the operational needs and requirements for practitioners in the field, steer the content of the document, address public comments, and assist with resolving various technical matters.

Through the American National Standards Institute (ANSI), NIJ supports U.S. operation of the secretariat for ISO/IEC JTC 1/SC 37 Biometrics, which focuses on the standardization of generic biometric technologies pertaining to human beings to support interoperability and data interchange among applications and systems.

USMS has not identified the need for any government unique standards in lieu of consensus-based standards. USMS Information Technology Division is represented in appropriate Standards Development Organizations along with other corresponding divisions and offices including, Office of General Council, CAPTURE Program, the Office of Data Governance, and Justice Prisoner Air Transportation System division. Collectively, they follow the policies of OMB Circular A-119 by regularly participating with commercial and private-sector on standard development of voluntary consensus standards via committees, working groups, meetings, conferences, and other engagements, including:

- **The International Standard for Business Aircraft Operations (IS-BAO):** The IS-BAO was developed by the business aviation community and is designed to promote use of high-quality operating practices by establishing a framework for effective safety and operational processes, providing tools to facilitate the implementation of best practices, and delivering a Safety Management System (SMS) appropriate to all operational profiles. IS-BAO helps operators apply industry best practices by challenging them to review and compare their safety-related policies, processes and procedures, and then make improvements, elevating them to the worldwide standard for business aviation.

The U.S. National Central Bureau (USNCB) is responsible for ensuring that its stewardship of INTERPOL data adheres to the Rules on Processing Data (RPD). INTERPOL's current RPD was adopted by INTERPOL's General Assembly (plenary session of all representatives from member countries) in 2011 and entered into force in July 2012. They have since been continually updated to keep pace with technological developments and evolving international data protection standards. The RPD was substantively updated at the General Assembly in 2024. The RPD govern all data processing in the INTERPOL Information System, including that surrounding the publication and circulation of Red Notices. This robust set of rules ensures the efficiency and quality of international cooperation between criminal police authorities through INTERPOL channels as well as due respect for the basic rights of the individuals who are subjects of this cooperation. USNCB has not created a derivative set of rules. The RPD is publicly available: https://www.interpol.int/content/download/5694/file/INTERPOL%20Rules%20on%20the%20Processing%20of%20Data-EN.pdf (will open as a pdf).

2. Please record any government-unique standards (GUS) your agency began using in lieu of voluntary consensus standards (VCS) during FY 2024. Please note, GUS which are still in effect from previous years should continue to be listed, and you do not need to report your agency's use of a GUS where no similar VCS exists.

Start by reviewing Table 1: Current Government Unique Standards FY2023.

To add a new GUS, please include:

1. **The name of the GUS;**
2. **The name(s) and version(s) of the VCS(s) that might have been used, but after review, found to be inappropriate;**
3. **A brief rationale on why the VCS(s) was not chosen.**

Current total GUS = 0

Table 1: Current Government Unique Standards FY2023