

Department of Justice (DOJ) Fiscal Year 2025 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 35 separate component organizations and has approximately 112,000 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, and 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 and 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 grantmaking functions.

The following summarizes some of DOJ's standards and conformity assessment activities in 2025, 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 on 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*.

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:

- **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, Firearms 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, Office of Justice Programs (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. These include 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 ATF, DEA, FBI, and JMD, the GCOI 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 Accelerator:** 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 ICAM 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. The Working Group gathers critical insights and information on the challenges of compliance, identifies opportunities, best-practices, and solutions to support compliance, and moves the Department forward toward securing IoT assets within the enterprise.

Other initiatives at the Component level include:

Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF)

The ATF Forensic Science Laboratories and the Fire Research Laboratory (FRL) are involved in numerous standards development organizations, including:

- The Organization of Scientific Area Committees for Forensic Science (OSAC),
- The American Society for Testing and Materials (ASTM),
- The Academy Standards Board (ASB),
- The National Fire Protection Association (NFPA),
- and the Scientific Working Group (SWG).

In FY2025, the FRL participated in the following committees:

- **Fire Investigations Committee:** managed NFPA 921, Guide for Fire and Explosives Investigations
- **Fire Investigator Professional Qualifications Committee:** managed NFPA 1033, Standard for Professional Qualifications for Fire Investigators
- **Fire Investigation Units Committee:** managed NFPA 1321, Standard for Fire Investigation Units.

As of September 30, 2025, these subcommittees have been discontinued by OSAC.

The ATF Laboratories are accredited by the ANSI National Accreditation Board (ANAB) to ISO 17025 and DNA QAS. The laboratories predominantly use internally developed and validated protocols. These protocols incorporate aspects of consensus documents generated by the forensic community. However, the laboratory includes supplemental requirements that exceed requirements in consensus documents or employ additional techniques not available to most forensic laboratories.

The Fire Research Laboratory (FRL) uses the consensus standard NFPA 289, which is the standard method of fire test for individual fuel packages.

The ATF Firearms and Ammunition Technology Division (FATD), within the Enforcement Programs and Services (EPS) Directorate, remains compliant within the scope of OMB Circular A-119 Revised *Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities* and the National Technology Transfer and Advancement Act (NTTAA - 15 U.S.C. § 3701 et seq. - 1996). FATD specifically complies with the requirement as stated in Circular A-119 Revised that established policies concerning the Federal Government development and use of voluntary consensus standards along with conformity assessment activities. The use of voluntary consensus standards is expected instead of using government-unique standards except where inconsistent with the law or deemed impractical.

The FATD Quality Manager is the ATF representative of DOJ on the American National Standards Institute Technical Advisory Group (ANSI US TAG) for the International Organization for Standardization Technical Committee 272, (ISO/TC 272), committed to the development of standards that pertain to laboratory and field based forensic science techniques and methodology in broad general areas such as the detection and collection of physical evidence, the subsequent analysis and interpretation of the evidence, and the reporting of results and findings. The most notable contribution of ISO/TC 272 is the publication of the 5-part series of ISO 21043 for evidence handling, analysis, interpretation and reporting.

The ATF National Integrated Ballistic Information Network (NIBIN) National Correlation and Training Center (NNCTC-1 and NNCTC-2) accreditation includes all personnel, equipment, and teams that constitute the NNCTC Program under the ISO/IEC 17020 standard (Conformity assessment – Requirements for the operation of various types of bodies performing inspection). The NNCTC conducts ballistics image correlations and returns investigative leads to more than 7,200 law enforcement agencies across the nation. This accounts for roughly 30% of all ballistic image acquisitions in the United States. Achieving accreditation from an independent, non-governmental, conformity assessment provider under this standard provides the NNCTC with external validation of its methods and standards of performance of testing and inspections. In addition, it results in formal recognition for competence to perform specific methods conducted by an independent third-party using a defined set of international standards.

ANSI is an independent, non-governmental accrediting organization accredited to perform this type of conformity assessment ISO/IEC 17020 – Conformity Assessment-Requirements for the Operation of Various Types of Bodies Performing Inspection and the 2023 ANAB ISO/IEC 17020:2012- Accreditation Requirements for Forensic Inspection (AR 3120).

Drug Enforcement Administration (DEA)

The DEA's Forensic Science Division (SF) ensures the DEA is represented in organizations involved in the development of voluntary consensus standards which apply to the forensic disciplines practiced by agency personnel, including:

- **American Society for Testing and Materials (ASTM) International:** In FY 2025, DEA had representation on ASTM's E30 Committee on Forensic Sciences, including one individual who served as both the Chair of the E30 Committee on Forensic Sciences and the Chair of the E30.16 Subcommittee on AI and Machine Learning in Forensic Science, and another individual who served as the chair of the E30.14 Subcommittee on Seized Drugs. Agency SMEs participated in task groups or as technical contacts in the development of standards. The DEA laboratory system is compliant with ASTM standards E2327-15, E2329-17, ASTM E2548-16, ASTM E2882-19, ASTM E2916-19, ASTM E2917-19a and ASTM E3255-21.
- **Organization of Scientific Area Committees for Forensic Science (OSAC):** In FY2025, DEA had representation on NIST's OSAC Seized Drug Subcommittee, including two individuals from SF who served as the subcommittee's Chair and Vice-Chair. Agency SMEs participated in several task groups, bringing together subject matter experts from across the country to review and update standards within the subcommittee for publication. The establishment of these standards strengthened the nation's use of forensic science by defining minimum requirements, best practices, standard protocols, and other guidance to help ensure that the results of forensic analysis are reliable and reproducible.
- **International Organization for Standardization (ISO) United States Technical Advisory Group - Technical Committee 272:** In FY2025, one forensic chemist participated in ISO/TC 272 and is involved in the development of standards that pertain to laboratory and field-based forensic science techniques and methodology in broad general areas such as the detection and collection of physical evidence, the subsequent analysis and interpretation of the evidence, and the reporting of results and findings.
- **Scientific Working Group for Seized Drugs (SWGDRUG):** In FY2025, DEA had representation on SWGDRUG, including one individual who served as the organization's Chair and one individual who served as Secretariat. Agency SMEs worked with a committee to revise the minimum recommendations, which are internationally accepted minimum standards that aim to improve the

quality of the forensic examination of seized drugs.

- **Scientific Working Group on Digital Evidence (SWGDE):** In FY2025, one digital evidence examiner represented DEA on SWGDE, which fosters communication, cooperation, consistency, and quality within the forensic community through consensus-based documents.

Federal Bureau of Investigation (FBI)

The FBI remains compliant in carrying 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 NTTAA. The Infrastructure Branch regularly participates in the following SDOs and bodies:

- **(U) Interagency Security Committee (ISC) Subcommittee:** The FBI participates in the Monthly ISC Subcommittee meetings with a focus on the cyber requirements for securing building automation systems, facility intrusion detection and surveillance, building access, and facility IoT for non-military federal facilities.
- **(U) Committee on National Security Systems (CNSS):** The FBI participates in CNSS meetings, focusing on the development of cybersecurity requirements for securing National Security Systems.
- **(U) Federal Acquisition Security Council (FASC):** The SECURE Technology Act of 2018 established the FASC to enhance government-wide coordination. The FASC is responsible for identifying supply chain risk management standards and guidelines, developing criteria for sharing information, engaging with private sector and non-government organizations (NGOs), coordinating with interagency committees, and providing recommendations on exclusions and/or removal orders. The FBI has representation across the council, Task Force(s), and working group(s) through a principal, deputy principal, staff lead, and legal counsel.
- **(U) IC Working Groups:** The OCIO participates in two key IC working groups on behalf of the FBI: the IC Joint Architecture Reference Model (JARM) and the IC Zero Trust Working Group (ZTWG). Both groups establish IC-level standards.

The Field Services Response Branch’s (FSRB) Operational Technology Division 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 Operational Technology Division follows 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 Operational Technology Division regularly participates in the following SDOs and bodies:

- **(U) International Telecommunications Union-Telecommunication Standardization Sector (ITU-T):** The FBI regularly attends ITU meetings. The ITU allocates global radio spectrum and satellite orbits, develops the technical standards that ensure networks and technologies seamlessly interconnect, and strives to improve access to Information Communication Technologies (ICT) to underserved communities worldwide. Standardization development and coinciding work is conducted via 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.
 - **(U) Study Group 21 (SG-21):** This study group is responsible for multimedia technologies and has assumed the lead in Artificial Intelligence studies around ICT.
- **(U) 3rd Generation Partnership Project (3GPP):** The FBI continues to participate in development of

service-based interception capabilities for 5G-based and evolving 6G 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):** ATIS is a standards organization that develops technical and operational standards and solutions for the ICT industry. The FBI continues to participate in the ATIS Packet Technology and Systems Committee and ATIS Lawfully Authorized Electronic Surveillance Committee.
- **(U) Internet Engineering Task Force (IETF):** IETF is an engineering group that develops technical standards of the internet's architecture, including encryption, cybersecurity, network security, routing, and other key protocols. The FBI continues to participate in this standards group 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):** ETSI is a standards development organization that develops global technical standards for ICT-enabled systems, applications, and services. The FBI continues to participate in the ETSI Technical Committee for Lawful Interception to satisfy the industry consultation requirements of CALEA for the development of industry lawful intercept specifications for covered services.
- **(U) Cable Television Laboratories, Inc. (CableLabs):** CableLabs is a standards development organization that develops global technical standards for broadband internet access services. The FBI continues to participate with CableLabs to satisfy the industry consultation requirements of CALEA for the development of industry lawful intercept specifications for covered services.
- **(U) Internet Corporation for Assigned Names and Numbers (ICANN):** ICANN is a global multistakeholder group responsible for coordinating the maintenance and procedures of several databases related to the namespaces and numerical spaces of the internet while also ensuring the internet's smooth, secure, and stable operation. The FBI continues to participate with ICANN to facilitate the development of policies governing how ICANN's contracted parties—domain registries and registrars—handle and disclose domain name registration data to law enforcement.

Office of the Inspector General (OIG)

The OIG Cyber Investigation Office (CIO) builds policies and procedures using Voluntary Consensus Standards and Standards Development Organizations (SDOs). DOJ OIG CIO follows both Voluntary Consensus Standards and SDOs and bodies to develop and exploit technology in the mission to investigate waste, fraud, and abuse. The DOJ OIG CIO has not identified the need for any government unique standards in lieu of consensus-based standards. Voluntary Consensus Standards and SDOs are also part of the fundamental basis for the Council of the Inspectors General on Integrity and Efficiency (CIGIE). CIGIE policies, guidelines and standards in conjunction with Voluntary Consensus Standards and Conformity Assessment Activities are the foundation for DOJ OIG Cyber Investigations Office operational procedures. The DOJ OIG Cyber Investigations Office regularly participates in the following Voluntary Consensus Standards, SDOs, and bodies:

Key Digital Forensic Governing and Standard-Setting Bodies:

Standards & Guidelines:

- **SWGDE (Scientific Working Group on Digital Evidence):** Focuses on developing consensus-based standards and guidelines for the digital forensic community.
- **NIST (National Institute of Standards and Technology):** Provides technical standards, guidelines, and testing for forensic tools (formerly involved in the NCFs).

Certification & Accreditation:

- **DFCB (Digital Forensics Certification Board):** A non-profit organization offering professional certifications like the DFCP, established through a National Institute of Justice cooperative agreement.
- **IACIS (International Association of Computer Investigative Specialists):** Provides globally recognized training and certification for computer forensic professionals.
- **GIAC (Global Information Assurance Certification):** Offers specialized certifications, such as GCCE and GCFA.

Governmental & Law Enforcement Bodies:

- **CIGIE (Council of the Inspectors General on Integrity and Efficiency):** Is an independent entity within the executive branch of the federal government of the United States established in October 2008 by the Inspector General Reform Act of 2008. The council addresses integrity, economy, and effectiveness issues that transcend individual government agencies; and increase the professionalism and effectiveness of personnel by developing policies, technical standards, and approaches to aid in the establishment of a well-trained and highly skilled workforce in the Office of Inspector General.
- **DC3 (Department of Defense Cyber Crime Center):** Serves as the DoD central agency for digital forensics, setting standards for criminal investigation.
- **NCFI (National Computer Forensics Institute):** Provides training to law enforcement, prosecutors, and judges.

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 operate its NIJ Compliance Testing Program (CTP), a conformity assessment program that provides third party certification of body armor worn by law enforcement officers. In FY 2025, NIJ implemented NIJ Standard 0101.07, *Ballistic Resistance of Body Armor*, through its NIJ CTP. The program received applications for 264 models of ballistic-resistant body armor submitted by 122 companies for eventual testing at five accredited commercial laboratories recognized by NIJ. NIJ Standard 0101.07 is a voluntary equipment performance standard for torso-worn body armor for law enforcement, which incorporates ten ASTM voluntary consensus standards (VCS), and updates the prior NIJ version. In FY2025, NIJ also implemented NIJ Standard 0123.00, *Specification for NIJ Ballistic Protection Levels and Associated Test Threats*, through its NIJ CTP. This standard is a voluntary specification that defines ballistic protection levels and associated test threats and incorporates three ASTM VCS. In FY2025, follow-up inspection and testing was conducted on 249 models complying with NIJ Standard 0101.06, *Ballistic*

Resistance of Body Armor. In addition, 6 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>.

United States Marshals Services (USMS)

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 Counsel, 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 the commercial and private sectors on the 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 were 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 were 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 are 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 list the government-unique standards your agency used in lieu of voluntary consensus standards during FY 2025:

- 2. Government Unique Standard: (name)**
 - 3. Voluntary Standard (that was not used): (name)**
 - 4. Rationale (for not using): (brief description)**
-