Department of Justice (DOJ) Fiscal Year 2022 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) comprises more than 40 separate component organizations and has approximately 116,000 employees who carry out the missions of its components. 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 DOJ mission is to enforce the law and defend the interests of the United States according to the law; to ensure public safety against threats foreign and domestic; to provide federal leadership in preventing and controlling crime; to seek just punishment for those guilty of unlawful behavior; and to ensure fair and impartial administration of justice for all Americans. DOJ is meeting these mission challenges through three strategic goals focused on advancing the Department's priorities and reflecting the outcomes the American people deserve. These goals are:

- Goal 1—Prevent Terrorism and Promote the Nation's Security Consistent with the Rule of Law;
- Goal 2—Prevent Crime, Protect the Rights of the American People, and Enforce Federal Law; and
- Goal 3—Ensure and Support the Fair, Impartial, Efficient, and Transparent Administration of Justice at the Federal, State, Local, Tribal, and International Levels.

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 2022, demonstrating the Department's active participation in improving and applying standards to deliver the mission.

The Federal Bureau of Investigation (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 National Technology Transfer and Advance Act (NTTAA). The FBI has not currently identified the need for any government unique standards in lieu of consensus-based standards.

The FBI's Science & Technology Branch (STB) 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. STB 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.

FBI-Science & Technology Branch (STB) regularly participates in the following SDOs and bodies:

- **Internet Corporation for Assigned Names and Numbers (ICANN**). International nonprofit responsible for the management of the Domain Name System (DNS). The FBI is an active, engaging participant in ICANN recurring meetings.
    - **Governmental Advisory Committee (GAC)**. An advisory committee to ICANN established via ICANN Bylaws and provides advice to ICANN on public policy aspects of ICANN's Domain Name System responsibilities. FBI participation provides direct access to the ICANN Board on public policy/LE-related issues. Enables early access to weigh in on development processes and ensure consistency with laws and national security interests. Provides access to experts across the national and international spectrum to engage on implications and mitigation strategies (if needed).
    - **Public Safety Working Group (PSWG)**. ICANN Governmental Advisory Committee (GAC) Working Group devoted to evaluating policies and procedures that implicate the safety of the public. Current strategies include developing DNS abuse and cybercrime mitigation capabilities of the ICANN and LE communities, preserving and improving domain registration directory services effectiveness, and leveraging stakeholders to influence balanced ICANN-level governance. The FBI directly contributed to development of a voluntary standard "framework"** for law enforcement referrals to domain registry operators of bulk lists of domain names linked to command and control of criminally operated botnets. Additionally, the FBI continues to provide public safety input to ongoing policy development for a replacement to the worldwide web's "WHOIS" system.
        - **Framework on Domain Generating Algorithms (DGAs) Associated with Malware and Botnets, link
- **International Telecommunications Union (ITU).** The FBI regularly attends meetings in ITU 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.

- **Internet Governance Forum (IGF).** The FBI continues 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).
    - **Internet Governance Forum USA (IGF-USA)**. The FBI continues to be an active participant in the IGF-USA recurring general meetings as well as working group meetings to illuminate issues and cultivate constructive discussions about the future of the internet.
- **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.
- **International Organization for Standardization (ISO)**. FBI is represented in the Committees/Working Groups of the ISO. ISO is an independent, non-governmental international organization with a membership of 167 national standards bodies. The ISO brings together experts to share knowledge and develop voluntary, consensus-based, market relevant International Standards that support innovation and provide solutions to global challenges.
- **International Committee for Information Technology Standards (INCITS).** FBI is represented in the Working Groups of the INCITS. INCITS is the central U.S. forum dedicated to creating technology standards for the next generation of innovation.
- **Iris Experts Group (IEG)** within the newly formed **Organization of Scientific Area Committees** - part of the **Facial Identification Subcommittee**. The IEG is a forum for the discussion of technical questions of interest to US government (USG) agencies and their staff that are employing or may employ iris recognition to carry out their mission. FBI continues to be represented. The **Facial Identification Subcommittee** focuses on standards and guidelines related to the image-based comparisons of human facial features.
- **ASTM E30 Committee on Forensic Sciences**. FBI-OTD SME chairs semi-annual meetings of E30 as well as meetings of the Executive Committee. The Committee has jurisdiction over 60 standards, published in the Annual Book of ASTM Standards, Volume 14.02. E30 has 5 technical subcommittees that manage these standards.
- **Organization of Scientific Area Committees for Forensic Science (OSAC).** FBI-OTD SME participated in (2) meetings of the OSAC FSSB Outreach task group, which is currently focused on engaging with forensic science stakeholders to adopt OSAC standards. The OSAC addresses a lack of discipline-specific forensic science standards. OSAC fills this gap by drafting proposed standards and sending them to SDOs which further develop and publish them.
    - **Digital Multimedia Scientific Area Committee (DMSAC)**. FBI serves as a member of DMSAC. The Committee sets development standards for forensic analysis of multimedia and digital evidence, to include image, video, audio/voice, and computer/digital data.
        - **Speaker Recognition Subcommittee (SR).** Works in the development of standards specific to forensic analysis of human voice data. The SR subcommittee reports to the DMSAC committee. FBI-OTD SME has served as the chair of SR for the past three years and conducts monthly meetings for the advancement of documents supporting the establishment of standards in forensic speaker recognition.
    - **National Information Exchange Model (NIEM).** FBI-OTD SME participates in bi-weekly meetings to advise the NIEM for the exchange of audio and voice information. The NIEM defines standard terminology, models, and relationships for the exchange of data across public and private organizations.

- **Telecommunications Industry Association (TIA) Engineering Committee (TR8).** FBI SMEs are represented and engage in TIA's work to formulate and maintain standards for private radio communications systems and equipment for both voice and data applications. TR-8 addresses all technical matters for systems and services, including definitions, interoperability, compatibility and compliance requirements.
- **APCO Project 25 Interface Committees (APIC).** FBI SMEs are represented. APIC is an ad hoc committee of the Private Radio Section (PRS) in the Wireless Communication Division (WCD) of the TIA. The APIC task groups are not standard formulating groups. The APIC task groups do develop documents that are reviewed by users and industry representatives, decisions based on consensus.
- **Federal Partnership for Interoperable Communications (FPIC).** Serves as a coordination and advisory body to address technical and operational wireless issues relative to interoperability within the public safety emergency communications community, interfacing with voluntary representatives from federal, state, local, territorial, and tribal organizations to include the FBI
    - **Federal Partnership for Interoperable Communications (FPIC) Security Subcommittee**. FBI SMEs are being represented. In coordination with the National Law Enforcement Communications Center (NLECC) and other public safety agencies, developed a standardized SLN assignment list for National Encrypted Interoperability.
- **Alliance for Telecommunications Industry Solutions (ATIS).** FBI participated in regard to 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.

- **Internet Engineering Task Force (IETF)**. Engineering group that develops technical standards of the internet's architecture including encryption, cybersecurity, network security, routing and other key protocols. The FBI has engaged over many years to build alliances. Primary attenders are industry along with academia and organizations such as NIST, NTIA, NSA, FBI and UK/NCSC.
- **SAFECOM**. FBI SMEs are represented. Through collaboration with emergency responders and elected officials across all levels of government, SAFECOM works to improve emergency response providers' inter-jurisdictional and interdisciplinary emergency communications interoperability across local, regional, tribal, state, territorial, international borders, and with federal government entities. SAFECOM works with existing federal communications programs and key emergency response stakeholders (to include the FBI) to address the need to develop better technologies and processes for the coordination of existing communications systems and future networks.
    - **National Council of Statewide Interoperability Coordinators (NCSWIC).** Established by the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA), the NCSWIC supports Statewide Interoperability Coordinators (SWIC) from the 56 states and territories, by developing products and services to assist them with leveraging their relationships, professional knowledge, and experience with public safety partners involved in interoperable communications at all levels of government to include the FBI.
- **3D Toolmark Technologies Technical Working Group (TWG).** FBI SMEs are represented. The TWG provides guidance and recommendations to the Firearms/Toolmarks community in instrument assessment and Virtual Comparison Microscopy (VCM). Creating standards for the F/T community to establish acceptable measuring practices, methodology/Standard Operating

Procedures (SOPs), and quality assurance protocols that can be utilized to access a laboratory's compliance during accreditation.

- **American Academy of Forensic Sciences-Academy Standards Board.** FBI SMEs are represented. SDO with the purpose of providing accessible, high-quality science-based consensus forensic standards.
- **American Society for Testing and Materials (ASTM) International.** FBI-LD SMEs are represented. International SDO that develops and publishes voluntary consensus technical standards for a wide range of materials, products, systems, and services.
- **International Society for Forensic Genetics.** FBI SMEs are represented. The society aims to promote scientific knowledge in the field of genetic markers as applied to forensic science. This is mainly being achieved through regular meetings regionally or internationally and their journal Forensic Science International: Genetics and the work of our expert DNA commissions.
- **National Fire Protection Association.** FBI SMEs are represented. International nonprofit organization in standards development devoted to eliminating death, injury, property and economic loss due to fire, electrical and related hazards.
- **Scientific Working Group-DNA Analysis Methods (SWGDAM).** FBI SMEs are represented. Serves as a forum to discuss, share, and evaluate forensic biology methods, protocols, training, and research to enhance forensic biology services as well as provide recommendations to the FBI Director on quality assurance standards for forensic DNA analysis.
- **Scientific Working Group-Seized Drugs (SWGDRUG).** FBI SMEs are represented. Maintains a database of reference mass spectra, or "molecular fingerprints" of controlled substances. This database is a cornerstone in the fight against illicit drugs, including newly emerging fentanyl analogues and other synthetic opioids. NIST scientists perform rigorous quality assurance on all new mass spectra added to the database, giving confidence to forensic chemists that the results they obtain using this database are accurate and reliable.
- **United States Technical Advisory Group-Technical Committee 272.** FBI SMEs are represented. The Committee is at the forefront of standardization and guidance in the field of Forensic Science. This includes 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 National Institute of Justice (NIJ) continues to operate its NIJ Compliance Testing Program. In calendar year (CY) 2022, over 90 models of ballistic-resistant body armor were submitted for testing. In addition to initial testing, follow-up inspection and testing was conducted on approximately 340 models complying with NIJ Standard 0101.06, Ballistic Resistance of Body Armor. NIJ continues to participate in ASTM International and National Fire Protection Association (NFPA) committees to develop standardized 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. Through ANSI, NIJ also supports 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. More about NIJ's standards and conformity assessment activities can be found at: https://nij.ojp.gov/equipment-standards-and-conformity-assessment.

The Department's Office of the Chief Information Officer actively applies the ISO 20000 and 27001

standards for the delivery of IT and information security services and has undergone formal audits to obtain ISO certification for compliance with these standards. The Department recertified its IT service management certification originally obtained in 2017 to the updated ISO/IEC 20000-1:2018 standard and achieved initial certification under the ISO 27001:2013 information security management standard. Application of these standards has significantly improved delivery of OCIO enterprise IT and cybersecurity services, ensuring the continuous evaluation of service performance and use of standard practices as defined by criteria well-recognized across industry and government.

2. Please keep track changes on to record or rescind any new government-unique standards (GUS) your agency began using in lieu of voluntary consensus standards (VCS) during FY 2022. 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 FY2022. If no changes, record the number of GUS in FY2022, save the file, and send to nrioux@nist.gov.

To add a new GUS, please go to Table 2: Government Unique Standards Added in FY2022 and use the template provided to add the GUS, VCS, and rationale. If more than one GUS is being added, please follow the template in listing any new GUS.

To rescind a GUS, (if they are no longer in use or have been replaced by a voluntary consensus standard) please cut the rescinded standard and paste in Table 3: Government Unique Standards Rescinded in FY2022. Please add a 'Rationale for Rescinding' explaining why the standard was rescinded.
Please record below the total number of GUS currently in use (previous years and new as of this FY). This number should include the previous total plus any new GUS added, and minus any GUS rescinded:
Number of GUS in FY2022: 0 + (new) - (rescinded) = 0

Table 1: Current Government Unique Standards FY2022