Federal Trade Commission
Privacy Impact Assessment

hG Sp Sn
(SG

R U

M 2023

1 System Overview 3
2 Data Type, Sources, and Use 5
3 Data Access and Sharing 8
4 Notice and Consent 9
5 Data Accuracy and Security 10
6 Data Retention and Disposal 11
7 Website Privacy Evaluation 12
8 Privacy Risks and Evaluation 12

1 [illegible]

1.1 [illegible]

The Federal Trade Commission (FTC, Commission, or Agency) is an independent federal law enforcement and regulatory agency with authority to promote consumer protection and competition through the prevention of unfair, deceptive, and anti-competitive business practices. The FTC pursues vigorous and effective law enforcement; advances consumer interests by sharing its expertise with federal and state legislatures and U.S. and international government agencies; develops policy and research tools through hearings, workshops, and conferences; and creates educational programs for consumers and businesses in a global marketplace with constantly changing technologies. The Commission enforces and administers a wide variety of competition and consumer protection laws.[1]

Agency employees and contractors operate out of offices in Washington, D.C., and regional offices located in Atlanta, Chicago, Cleveland, Dallas, Los Angeles, New York, San Francisco, and Seattle. The Bureaus of Consumer Protection (BCP), Competition (BC), and Economics (BE) conduct the FTC's mission-related work. The Office of General Counsel (OGC) provides legal counsel to Bureaus and handles most appellate litigation. The Office of the Chief Information Officer (OCIO) operates and maintains the necessary Information Technology (IT) services to support the mission, including the network, servers, applications, databases, computers, and communication facilities.

The FTC General Support System (GSS) is the FTC's primary IT infrastructure to host information systems that collect, process, disseminate, and store information in support of the Agency's mission. It is a collection of FTC systems protected by a common set of security controls. The GSS supports the major administrative and mission functions of the Agency and provides for the internal and external transmission and storage of Agency data. It is the IT platform or host for a number of FTC systems of records covered by the Privacy Act of 1974, 5 U.S.C. § 552a.[2] The GSS encompasses all permanent FTC locations and approved remote connections. The OCIO is the business owner for the GSS.

The GSS has dedicated connections with external (non-FTC) entities as necessary to support the FTC mission. Those connections are:

[illegible]	[illegible]
Department of Interior, Interior Business Center (Denver)	Financial & Human Resources management
Department of Justice	HSR Electronic Filing System and Cyber Security Assessment and Management (CSAM)

[1] A list of the statutes enforced or administered by the FTC is available at

2.3 How is the purpose of the system and the information to be collected, used, disseminated, and maintained for the Commission to perform its law enforcement, policy, personnel management, and other activities. FTC staff members collect and use the information to investigate anti-competitive practices and to enforce statutes protecting consumers from fraudulent, deceptive, and unfair acts and practices in the marketplace. FTC staff also use the information

Typically, information is obtained directly from targets of the FTC's law enforcement activities and from individuals and entities with information that may be relevant to an FTC investigation. Information is generally collected directly from whatever media is used to submit it. This may include copying information from paper-based sources or from removable media such as CDs, DVDs, and hard drives. It may also include copying information that is electronically submitted via the Agency's Secure File Transfer System, email, or other electronic submission mechanism (e.g., through a website form).

Information also may be collected by the FTC, its contractors, and law enforcement partners through a court-sanctioned immediate access, which involves entering the premises where the information is stored and using specialized computer equipment and software to copy the information to removable media (typically hard drives). Information may also .lso .l0-6 (l)-6 Tc Tc 0 .(59-2

3.3 If you wish to modify the 3.2, the

development. Disposition of general technology management records and information system security records is authorized under National Archives and Records Administration (NARA) General Records Schedules 3.1 and 3.2.

7 [illegible]

7.1 [illegible]

Any tracking technologies used [illegible]

Risk	*Mitigation Strategy*
Unapproved Sensitive PII Storage	To address this risk, FTC policy states that electronic documents (including emails) containing Sensitive PII may be stored only on individually assigned FTC network storage space, on a shared FTC network drive in an access-restricted file folder, or FTC-provided device.
Lost or Misplaced Tape Backup Media	To address this risk, the FTC encrypts all GSS data stored on NetApp backup storage appliance.

8.4 [illegible]

The collection, use, and disclosure of information in this system are consistent with the FTC's Privacy Policy. Access logs, storage logs, and firewall logs are periodically reviewed to ensure that users are complying with GSS policies and procedures. In addition, all FTC staff and contractors must review and sign the FTC Rules of Behavior form on an annual basis.