U.S. Consumer Product Safety Commission
PRIVACY IMPACT ASSESSMENT

Name of Project:	GSS LAN
Office/Directorate:	EXIT/ITTS

A. CONTACT INFORMATION

Person completing PIA: (Name, title, organization and ext.)	Terry Bard, Director, ITTS
System Owner: (Name, title, organization and ext.)	Terry Bard, Director, ITTS
System Manager: (Name, title, organization and ext.)	Denis Suski, Chief Network Engineering Branch, ITTS/TSNE, x6724

B. APPROVING OFFICIALS	Signature	Approve	Disapprove	Date
System Owner	TERRY BARD Digitally signed by TERRY BARD DN: c=US, o=U.S. Government, ou=Consumer Product Safety Commission, cn=TERRY BARD, 0.9.2342.19200300.100.1.1=61001000000925 Date: 2018.09.10 04:43:59 -04'00' Terry Bard, ITTS	☑	□	9/10/18
Privacy Advocate	PATRICK MANLEY Digitally signed by PATRICK MANLEY DN: c=US, o=U.S. Government, ou=Consumer Product Safety Commission, cn=PATRICK MANLEY, 0.9.2342.19200300.100.1.1=61001000000929 Date: 2018.09.06 16:21:00 -04'00' Patrick Manley, ITSO	☑	□	9/6/18
Chief Information Security Officer	PATRICK MANLEY Digitally signed by PATRICK MANLEY DN: c=US, o=U.S. Government, ou=Consumer Product Safety Commission, cn=PATRICK MANLEY, 0.9.2342.19200300.100.1.1=61001000000929 Date: 2018.09.06 16:21:36 -04'00' Patrick Manley, ITSO	☑	□	9/6/18
Senior Agency Official for Privacy System of Record? ______Yes __X___No	JAMES ROLFES Digitally signed by JAMES ROLFES DN: c=US, o=U.S. Government, ou=Consumer Product Safety Commission, cn=JAMES ROLFES, 0.9.2342.19200300.100.1.1=61001001116382 Date: 2018.09.12 09:38:20 -04'00' James Rolfes, SAOP/CIO	☑	□	9/12/18
Reviewing Official:	JAMES ROLFES Digitally signed by JAMES ROLFES DN: c=US, o=U.S. Government, ou=Consumer Product Safety Commission, cn=JAMES ROLFES, 0.9.2342.19200300.100.1.1=61001001116382 Date: 2018.09.12 09:40:33 -04'00' James Rolfes, SAOP/CIO	☑	□	9/12/18

C. SYSTEM APPLICATION/GENERAL INFORMATION

1. Does this system contain any personal information about individuals? (If there is NO information collected, maintained, or used that is identifiable to the individual, the remainder of PIA does not have to be completed.)	Yes. This system is a GSS LAN designed to transport information and provide general file storage. File storage may contained personal information about individuals. The customers of the GSS LAN are predominately CPSC employees and contractors who use the system for administrative purposes.
2. Is this an electronic system?	Yes

D. DATA IN THE SYSTEM	
1. What categories of individuals are covered in the system? (public, employees, contractors)	Public, Employee, Contractors
2. Generally describe what data/information will be collected in the system.	The GSS LAN supports individual CPSC data systems that may contain personally identifiable information such as information from the public, procurement, and personal and financial information regarding employees and contractors.
3. Is the source of the information from the individual or is it taken from another source? If not directly from individual, then what other source?	See individual PIAs for each specific data system.
4. How will data be checked for completeness?	See individual PIAs for each specific data system.
5. Is the data current? (What steps or procedures are taken to ensure the data is current and not out-of-date?)	See individual PIAs for each specific data system.
6. Are the data elements described in detail and documented? (If yes, what is the name and location of the document?)	See individual PIAs for each specific data system.
E. ATTRIBUTES OF THE DATA	
1. Explain how the use of the data is both relevant and necessary to the purpose for which the system is being designed?	Records that contain PII are only maintained if they are relevant and necessary to accomplish the agency mission. See individual PIAs for each specific data system.
2. For electronic systems, if the data is being consolidated, what controls are in place to protect the data from unauthorized access or use? Explain.	Access to the GSS LAN is controlled two-factor smartcard authentication. Rights to individual folders are controlled by group membership and granted on a need to know basis.
3. How will the data be retrieved? Can it be retrieved by a personal identifier? If yes, explain and list the identifiers that will be used to retrieve information on the individual.	Data is transmitted and stored in many unstructured file systems that may contain personal identifiers. See individual PIAs for each specific data system.
4. What opportunities do individuals have to decline to provide information or to consent to particular uses of the information?	In consumer complaint, Hotline, FOIA data systems, individuals are given the option to provide the data or not. See individual PIAs for each specific data system.
F. MAINTENANCE AND ADMINISTRATIVE CONTROLS	
1. What are the retention periods of data in this system?	CPSC follows NARA records schedules for data retention.
2. What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?	CPSC follows established schedules for retention and destruction of data.
3. For electronic systems, will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.	No. See individual PIAs for each specific data system.
4. For electronic systems only, what	Access to the GSS is controlled by two-factor smartcard authentication. Rights to

controls will be used to prevent unauthorized monitoring?	individual folders are controlled by group membership and granted on a need to know basis. Access Control List limits only authorized users' access to records.
5. Is this system currently identified as a CPSC system of records? If so, under which notice does the system operate?	NO. The GSS LAN itself does not contain PII, however, individual data systems may and may have associated SORNs.
6. If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain	No.

G. ACCESS TO DATA

1. Who will have access to the data in the system? (e.g., contractors, managers, system administrators, developers, other).	Contractors, managers, system administrators, developers, owners.
2. What controls are in place to prevent the misuse of data by those having access? (Please list processes and training materials.)	Rules of Behavior documents, written IT policy, annual security and privacy training.
3. Who is responsible for assuring proper use of the data?	Data owners for each individual data system.
4. Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? Are contractors involved in the collection of the data? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?	Contractors may be involved in the design and development of data systems. See individual PIAs. Privacy Act contract clauses are routinely inserted into CPSC contracts.
5. Do other systems share data or have access to the data in the system? If yes, explain. Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?	Only CPSC maintained systems share data with the GSS LAN.
6. Will other agencies share data or have access to the data in this system? If yes, how will the data be used by the other agency?	No
7. Will any of the personally identifiable information be accessed remotely or physically removed?	Yes, individual data systems can be remotely accessed. Remote access is granted only to approved users who authenticate using two-factor authentication over FIPS 140-2 compliant encrypted tunnels.