



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

SLATER (SLATER)

Department of the Navy - NAVRESFOR

### **SECTION 1: IS A PIA REQUIRED?**

**a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).**

- (1) Yes, from members of the general public.
- (2) Yes, from Federal personnel\* and/or Federal contractors.
- (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.
- (4) No

\* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

**b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.**

**c. If "Yes," then a PIA is required. Proceed to Section 2.**

**SECTION 2: PIA SUMMARY INFORMATION**

**a. Why is this PIA being created or updated? Choose one:**

- New DoD Information System**
- Existing DoD Information System**
- Significantly Modified DoD Information System**
- New Electronic Collection**
- Existing Electronic Collection**

**b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?**

- Yes, DITPR**      Enter DITPR System Identification Number
- Yes, SIPRNET**      Enter SIPRNET Identification Number
- No**

**c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?**

- Yes**       **No**
- If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

**d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?**

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

- Yes**       **No**
- If "Yes," enter Privacy Act SORN Identifier

DoD Component-assigned designator, not the Federal Register number.  
Consult the Component Privacy Office for additional information or  
access DoD Privacy Act SORNs at: <http://www.defenselink.mil/privacy/notices/>

or

**Date of submission for approval to Defense Privacy Office**        
Consult the Component Privacy Office for this date.

**e. Does this DoD information system or electronic collection have an OMB Control Number?**

Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

**Yes**

**Enter OMB Control Number**

**Enter Expiration Date**

**No**

**f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.**

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority (“internal housekeeping”) as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

SORN Authorities:

5 U.S.C. 301, Department Regulations;  
DoD 6025.18-R, DoD Health Information Privacy Regulation;  
and E.O. 9397 (SSN), as amended

Other Authorities:

10 U.S.C. 5013, Department of the Navy  
10 U.S.C. Subtitle E, Reserve Components  
1007, Administration of Reserve Components  
BUPERS Instruction 1001.39F, Administration Procedures for Navy Personnel  
OPNAV Instruction 100.16K, Navy Total Force Manpower Policies and Procedures

**g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.**

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

SLATER – Standalone supports the Navy Reserve Forces (NAVRESFOR) Annual Navy Reserve National Command and Senior Officer (05/06) Non-command Billet Screening and Assignment Board process. This process is only available for a specific period of time each year as designated by the Executive Steering Committee (ESC). Assigning the best qualified officers to senior leadership and management positions is vital to the continued successful support provided to the Active Component supported commands. This is achieved through a consistent screening and assignment process which promotes credibility with Resource Sponsors, Major Claimants, Supported Commands and the Selected Reserve Community. In order to provide consistent vetting of applicant qualifications and eligibility, all Reserve Component communities will participate in the APPLY Board. SLATER – Standalone is a non-GIG-connected, non-public-facing system used by the Navy Reserve National Command and Senior Officer (05/06) Non-Command Billet Screening and Assignment APPLY Board members to ultimately assign billets to the most qualified officer. It provides Navy Personnel Command (NPC) ranking data on Selected Reservists (SELRES) and NAVRESFOR billet preference data which is used by a panel of reserve community leaders to determine which reservists are assigned to which command billets.

Personal information collected: Name, SSN, Citizenship, Gender, Race/Ethnicity, Birth Date, Mailing/Home Address, Personal/Work Email, Security Clearance, Marital Status, Military Records, Education Information: education level/major/speciality code, high school diploma or GED and years of education; Other: SLATER - Standalone stores records reflecting information pertaining to the individual's participation in the Reserves and personal information collected such as Military Record Information: rank/grade and other pertinent information related to recruitment, classification, assignment, retention, reenlistment, promotion, advancement, training, education, professional history, experience, performance, qualifications, retirement, orders and administration SELRES.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

The disclosure of the information stored in the SLATER - Standalone could lead to identity theft/fraud or perhaps be used to target individuals for exploitation. The data stored in the SLATER - Standalone is protected by a variety of methods. Access to the data is restricted to authorized users only. All system users are required to undergo annual Privacy Act and Information Assurance (IA) training.

The SLATER – Standalone system is in a closed environment and it is not interconnected to any other network. It is a standalone, non-GIG connected, non-public facing configuration system. The system does not transmit, receive, route or exchange information outside of the closed environment. It is not PKI enabled. Privacy risks are highly unlikely.

**h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.**

**Within the DoD Component.**

Specify.

**Other DoD Components.**

Specify.

**Other Federal Agencies.**

Specify.

**State and Local Agencies.**

Specify.

**Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify.

CACI, Inc.

The contractor shall have an operational security program in strict compliance with the National Industrial Security Program Operating Manual (Department of Defense (DoD) 5220.22-M) and Space and Naval Warfare Systems Center, Atlantic (SSCA) security directives at the time of award. Clearance is required to access and handle classified and personal personnel material, attend program meetings, and/or work within restricted areas unescorted.

If contractor personnel require access to any Navy IT systems or resources at SSCA (directly or indirectly), all contractor personnel shall be required to complete the mandatory annual IA training and submit a signed System Authorization Access Request Navy (SAAR-N) form to the contract's specified Contracting Officer's Representative (COR).

The contractor shall demonstrate expertise in supporting and complying with DoN and DoD enterprise initiatives that include Personally Identifiable Information (PII).

The Contractor shall conform to the provisions of DOD 5220.22M, SECNAVINST 5510.30, and the Privacy Act of 1974.

Contractor personnel shall sign a Non-Disclosure Agreement when tasking requires access to PII.

**Other** (e.g., commercial providers, colleges).

Specify.

**i. Do individuals have the opportunity to object to the collection of their PII?**

**Yes**

**No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object.

This system will not be the initial collection point of PII, but may be used as follow-on or archival storage. As such, the individuals have already agreed to the collection of their PII via the primary collection system.

**j. Do individuals have the opportunity to consent to the specific uses of their PII?**

- Yes                                       No

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

PII is not solicited from the individual by SLATER - Standalone. PII is collected by the authoritative source systems and securely transferred to SLATER - Standalone on a periodic basis.

**k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.**

- Privacy Act Statement                       Privacy Advisory  
 Other     None

Describe each applicable format.

SLATER – Standalone supports the Navy Reserve Forces (NAVRESFOR) Annual Navy Reserve National Command and Senior Officer (05/06) Non-command Billet Screening and Assignment Board process. SLATER - Standalone stores data it receives via sneaker-net with the various authoritative source systems. Individuals are never asked to provide PII to SLATER - Standalone. The PII data contained in SLATER - Standalone is supplied by authoritative source systems. The authoritative source systems collecting the PII has the responsibility of providing the individual with any information related to the collection of PII.

--

**NOTE:**

**Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.**

**A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.**

**SECTION 3: PIA QUESTIONNAIRE and RISK REVIEW**

a. For the questions in subparagraphs 3.a.(1) through 3.a.(5), indicate what PII (a data element alone or in combination that can uniquely identify an individual) will be collected and describe the source, collection method, purpose, and intended use of the PII.

**(1) What PII will be collected?** Indicate all individual PII or PII groupings that apply below.

- Name  Other Names Used  Social Security Number (SSN)
- Truncated SSN  Driver's License  Other ID Number
- Citizenship  Legal Status  Gender
- Race/Ethnicity  Birth Date  Place of Birth
- Personal Cell Telephone Number  Home Telephone Number  Personal Email Address
- Mailing/Home Address  Religious Preference  Security Clearance
- Mother's Maiden Name  Mother's Middle Name  Spouse Information
- Marital Status  Biometrics  Child Information
- Financial Information  Medical Information  Disability Information
- Law Enforcement Information  Employment Information  Military Records
- Emergency Contact  Education Information  Other

If "Other," specify or explain any PII grouping selected.

Other: SLATER - Standalone stores records reflecting information pertaining to the individual's participation in the Reserves and personal information collected such as Military Record Information: rank/grade, work email, and other pertinent information related to recruitment, classification, assignment, retention, reenlistment, promotion, advancement, training, education, professional history, experience, performance, qualifications, retirement, orders and administration SELRES.  
 Education Information includes: education level/major/speciality code, high school diploma or GED and years of education.

**(2) What is the source for the PII collected (e.g., individual, existing DoD information systems, other Federal information systems or databases, commercial systems)?**

DoD/DON information systems: Navy Reserve Data Warehouse - Decision Support System (NRDW - DSS) (DITPR-DON #20931) and Navy Reserve Homeport (NRH) DITPR-DON #20932

**(3) How will the information be collected?** Indicate all that apply.

- Paper Form
- Telephone Interview
- Email
- Information Sharing - System to System
- Other
- Face-to-Face Contact
- Fax
- Web Site

**(4) Why are you collecting the PII selected (e.g., verification, identification, authentication, data matching)?**

SLATER - Standalone stores PII data in order to be able to verify the status of the Navy Reserve Forces for the purpose of providing leadership with an accurate assessment of readiness and to assist in the command's operational support decision-making.

**(5) What is the intended use of the PII collected (e.g., mission-related use, administrative use)?**

Mission-related use: Supports mission capability and readiness.

**b. Does this DoD information system or electronic collection create or derive new PII about individuals through data aggregation?** (See Appendix for data aggregation definition.)

- Yes
- No

If "Yes," explain what risks are introduced by this data aggregation and how this risk is mitigated.

**c. Who has or will have access to PII in this DoD information system or electronic collection?** Indicate all that apply.

- Users**
- Developers**
- System Administrators**
- Contractors**
  
- Other**

Developers and on-site contractors will have access to PII as part of their operational duties. Privileged Access Authorization (PAA) agreements are required for all privileged users. All access via Government Furnished Equipment (GFE) with all required IA controls and data encryption at rest capability.

**d. How will the PII be secured?**

**(1) Physical controls.** Indicate all that apply.

- Security Guards**
- Identification Badges**
- Key Cards**
- Safes**
- Cipher Locks**
- Combination Locks**
- Closed Circuit TV (CCTV)**
- Other**

**(2) Technical Controls.** Indicate all that apply.

- User Identification**
- Password**
- Intrusion Detection System (IDS)**
- Encryption**
- External Certificate Authority (CA) Certificate**
- Other**
- Biometrics**
- Firewall**
- Virtual Private Network (VPN)**
- DoD Public Key Infrastructure Certificates**
- Common Access Card (CAC)**

The SLATER – Standalone system is in a closed environment and it is not interconnected to any other network. It is a standalone, non-GIG connected, non-public facing configuration system. The system does not transmit, receive, route or exchange information outside of the closed environment. It is not Public Key Infrastructure (PKI) enabled.

**(3) Administrative Controls.** Indicate all that apply.

- Periodic Security Audits**
- Regular Monitoring of Users' Security Practices**
- Methods to Ensure Only Authorized Personnel Access to PII**
- Encryption of Backups Containing Sensitive Data**
- Backups Secured Off-site**
- Other**

Personnel will be trained to ensure they follow DoD/DON and federal guidelines regarding PII.

**e. Does this DoD information system require certification and accreditation under the DoD Information Assurance Certification and Accreditation Process (DIACAP)?**

**Yes. Indicate the certification and accreditation status:**

- |                                     |  |                      |                       |
|-------------------------------------|--|----------------------|-----------------------|
| <input checked="" type="checkbox"/> | <b>Authorization to Operate (ATO)</b>            | <b>Date Granted:</b> | Currently in progress |
| <input type="checkbox"/>            | <b>Interim Authorization to Operate (IATO)</b>   | <b>Date Granted:</b> |                       |
| <input type="checkbox"/>            | <b>Denial of Authorization to Operate (DATO)</b> | <b>Date Granted:</b> |                       |
| <input type="checkbox"/>            | <b>Interim Authorization to Test (IATT)</b>      | <b>Date Granted:</b> |                       |

**No, this DoD information system does not require certification and accreditation.**

**f. How do information handling practices at each stage of the "information life cycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individuals' privacy?**

DoD guidelines and best practices are utilized during all phases of the life cycle. Only the minimum amount of information required is collected, used and retained. Data is encrypted during processing and at rest where allowed. Information is deleted when no longer required.

Collection: PII provided via the system to system (with the authoritative source systems) interfaces using a VPN, secure file gateway, or secure network interface.

Use, Retention, and Processing: Only personnel with the "need-to-know" can access an individual's PII information.

Disclosure: Only personnel with the "need-to-know" can access an individual's PII information.

**g. For existing DoD information systems or electronic collections, what measures have been put in place to address identified privacy risks?**

The perceived threats are primarily computer hackers and disgruntled employees, state sponsored information warfare, and acts of nature. All systems are at risk because they may be vulnerable to unauthorized intrusion and hacking.

Since SLATER - Standalone operates in a non-GIG-connected, non-public-facing closed environment, there exists a possibility that security controls could be disabled for maintenance and other purposes. The risk would be that the security controls would not be reset.

All systems are vulnerable to "insider threats". SLATER - Standalone system administrators reduce the likelihood of this threat occurring by limiting system access to those individuals who have a defined need to access the information. There are defined criteria to identify who should have access to SLATER - Standalone. These individuals have gone through extensive background and employment investigations.

Mitigation:

The following controls are used to mitigate privacy risks:

1) Access Controls: Access to the closed environment and the specific functional areas of the system is limited by a combination of access controls. Naval Reserve Forces (NAVRESFOR) will employ technical, physical, personnel and procedural security, environmental protection and communications security to provide protection adequate to handle, control, process and store information in order to ensure compliance and availability. Commander, Naval Reserve Forces Command (CNRFC) Program Office limits the number of personnel with privileged access to the operational minimum required.

2) Confidentiality: Data is encrypted when possible to ensure that data is not made available or disclosed to unauthorized individuals, entities, or processes. Database views and export restrictions are enforced on the database. User access restrictions aid in maintaining data confidentiality.

3) Integrity: Limiting user access to data through the enforcement of the principles of "need-to-know" and "least privileges" minimizes the threat of unauthorized data alteration or destruction. All appropriate NIST 800-53 security and privacy controls for a "Medium" system have been implemented.

4) Audits: NAVRESFOR manages the review and examination of records, activities, and system parameters, to assess the adequacy of maintaining and controlling events that may degrade the security posture of SLATER - Standalone. Activity/system auditing and logging assess and record the security posture. System and database administrators monitor user action/event logs and review security reports generated by the system.

5) Training: All users are required to complete PII and IA training prior to being granted a SLATER - Standalone user account. In addition, system and database administrators are required to meet 8570.01M IA requirements before being granted elevated privileges.

SLATER - Standalone is located at Navy Personnel Command, Millington Navy Base. The Social Security Number Reduction Justification Memo is valid.

**h. For new DoD information systems or electronic collections, what measures are planned for implementation to address identified privacy risks?**

N/A



## SECTION 4: REVIEW AND APPROVAL SIGNATURES

Prior to the submission of the PIA for review and approval, the PIA must be coordinated by the Program Manager or designee through the Information Assurance Manager and Privacy Representative at the local level.

### **Program Manager or Designee Signature**

HALL.THOMAS.J.JR.1042503920  
Digitally signed by HALL.THOMAS.J.JR.1042503920  
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USN,  
cn=HALL.THOMAS.J.JR.1042503920  
Date: 2015.03.25 13:14:34 -04'00'

Name: LCDR Thomas J. Hall

Title: SLATER - Standalone Program Manager

Organization: Commander, Navy Reserve Forces Command

Work Telephone Number: (757) 444-3913

DSN:

Email Address: THOMAS.J.HALL1@NAVY.MIL

Date of Review: 25MAR15

### **Other Official Signature (to be used at Component discretion)**

JOHNSTON.KEVIN.LEE.1  
239171270  
Digitally signed by JOHNSTON.KEVIN.LEE.1239171270  
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI,  
ou=USN, cn=JOHNSTON.KEVIN.LEE.1239171270  
Date: 2015.03.26 08:22:56 -04'00'

Name: LCDR Kevin L. Johnston

Title: CNRFC N64 - Information Assurance Manager

Organization: Commander, Navy Reserve Forces Command

Work Telephone Number: (757) 322-6670

DSN: (757) 262-6670

Email Address: kevin.l.johnston@navy.mil

Date of Review: 25MAR15

**Other Official Signature  
(to be used at Component  
discretion)**

**WADSWORTH.CLINTON**  
**.D.1154469245**  
Digitally signed by WADSWORTH.CLINTON.D.1154469245  
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USN,  
cn=WADSWORTH.CLINTON.D.1154469245  
Date: 2015.03.26 05:51:17 -04'00'

Name: Mr. Clinton Wadsworth  
Title: CNRFC N6 - Deputy Chief Technology Officer  
Organization: Commander, Navy Reserve Forces Command  
Work Telephone Number: (757) 322-6643  
DSN: (757) 262-6643  
Email Address: clinton.wadsworth@navy.mil  
Date of Review: 3/25/2015

**Component Senior  
Information Assurance  
Officer Signature or  
Designee**

**HOWARD.DAVID.WI**  
**LLIAM.1154982520**  
Digitally signed by  
HOWARD.DAVID.WILLIAM.1154982520  
DN: c=US, o=U.S. Government, ou=DoD,  
ou=PKI, ou=USN,  
cn=HOWARD.DAVID.WILLIAM.1154982520  
Date: 2015.03.26 08:14:18 -04'00'

Name: CAPT David W. Howard  
Title: CNRFC N6 - Chief Technology Officer  
Organization: Commander, Navy Reserve Forces Command  
Work Telephone Number: (757) 322-6645  
DSN: (757) 262-6645  
Email Address: david.w.howard@navy.mil  
Date of Review: 3/25/2015

**Component Privacy Officer  
Signature**

**PATTERSON.ROBIN.W.1229**  
**323403**  
Digitally signed by PATTERSON.ROBIN.W.1229323403  
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI,  
ou=USN, cn=PATTERSON.ROBIN.W.1229323403  
Date: 2015.05.08 14:26:17 -04'00'

Name: Robin Patterson  
Title: Head, FOIA/Privacy Act Program Office (OPNAV DNS-36)  
Organization: Office of the Chief of Naval Operations (CNO)  
Work Telephone Number: 202-685-6545  
DSN:  
Email Address: robin.patterson@navy.mil  
Date of Review:

**Component CIO Signature  
(Reviewing Official)**

**MUCK.STEVEN.ROBERT.1179488597**  
Digitally signed by MUCK.STEVEN.ROBERT.1179488597  
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI,  
ou=USN, cn=MUCK.STEVEN.ROBERT.1179488597  
Date: 2015.05.13 15:02:40 -04'00'

Name:	for Lynda Pierce
Title:	Principal Deputy CIO
Organization:	Office of the Department of the Navy Chief Information Officer (DON CIO)
Work Telephone Number:	703-695-1842
DSN:	
Email Address:	lynda.pierce@navy.mil
Date of Review:	13 May 2015

**Publishing:**

Only Sections 1 and 2 of this PIA will be published. Each DoD Component will maintain a central repository of PIAs on the Component's public Web site. DoD Components will submit an electronic copy of each approved PIA to the DoD CIO at: [pia@osd.mil](mailto:pia@osd.mil).

If the PIA document contains information that would reveal sensitive information or raise security concerns, the DoD Component may restrict the publication of the assessment to include Sections 1 and 2.

## APPENDIX

Data Aggregation. Any process in which information is gathered and expressed in a summary form for purposes such as statistical analysis. A common aggregation purpose is to compile information about particular groups based on specific variables such as age, profession, or income.

DoD Information System. A set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes automated information system (AIS) applications, enclaves, outsourced information technology (IT)-based processes and platform IT interconnections.

Electronic Collection. Any collection of information enabled by IT.

Federal Personnel. Officers and employees of the Government of the United States, members of the uniformed services (including members of the Reserve Components), and individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the United States (including survivor benefits). For the purposes of PIAs, DoD dependents are considered members of the general public.

Personally Identifiable Information (PII). Information about an individual that identifies, links, relates or is unique to, or describes him or her (e.g., a social security number; age; marital status; race; salary; home telephone number; other demographic, biometric, personnel, medical, and financial information). Also, information that can be used to distinguish or trace an individual's identity, such as his or her name; social security number; date and place of birth; mother's maiden name; and biometric records, including any other personal information that is linked or linkable to a specified individual.

Privacy Act Statements. When an individual is requested to furnish personal information about himself or herself for inclusion in a system of records, providing a Privacy Act statement is required to enable the individual to make an informed decision whether to provide the information requested.

Privacy Advisory. A notification informing an individual as to why information is being solicited and how such information will be used. If PII is solicited by a DoD Web site (e.g., collected as part of an email feedback/ comments feature on a Web site) and the information is not maintained in a Privacy Act system of records, the solicitation of such information triggers the requirement for a privacy advisory (PA).

System of Records Notice (SORN). Public notice of the existence and character of a group of records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. The Privacy Act of 1974 requires this notice to be published in the Federal Register upon establishment or substantive revision of the system, and establishes what information about the system must be included.