BPA Policy 470-3

Protection of Personally Identifiable Information Within the BPA Application Portfolio

Table of Contents

1. Purpose & Background

To establish requirements, assign responsibilities, and provide guidance to meet Cyber Security requirements for the protection and incident reporting pertaining to Personally Identifiable Information (PII) within BPA's Information Technology (IT) systems.

2. Policy Owner

The BPA Chief Information Officer (CIO) is the owner of this policy.

3. Applicability

All organizations and staff within BPA, regardless of geographical location or purpose, are required to adhere to this policy.

This policy applies to all data identified as PII and the personnel who have authorized access to BPA systems using PII data. Scope is determined by two criteria: (1) PII that is removed from or (2) accessed outside of the physical BPA security boundary (OMB M-06-16, June 23, 2006).

This policy does not override the conditions outlined in BPA policy regarding the business use of BPA information technology services, or the Freedom of Information Act.

4. Terms & Definitions

A. **Information Technology (Title 40 US Code, Section 11101),** with respect to an executive agency means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use—

1. of that equipment; or
2. of that equipment to a significant extent in the performance of a service or the furnishing of a product;

It includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources. All IP-addressable equipment or devices are included in this category.

B. **BPA IT Equipment,** includes but is not limited to BPA's computer networks and any authorized BPA-owned or leased computing device or component that can be attached or connected to BPA's computer network, including any IP-addressable equipment or devices. BPA IT Equipment includes desktop computers and monitors, laptop and portable computers, tablets, thin clients and mobile thin clients, firmware, software, shareware, freeware, personal digital assistants (PDAs), telephones, digital cameras, cell phones, smart phones, facsimile machines, pagers, copiers, photocopiers, printers, scanners, servers, fixed or portable storage devices (e.g. flash drives), routers, peripheral devices, multi-purpose machines (e.g. combined facsimile, printer, and copier), and cloud-based IT services such as Archive-as-a-Service, Storage-as-a-Service, Desktop-as-a-Service, Software-as-a-Service, Platform-as-a-Service, Infrastructure-as-a-Service, Backup-as-a-Service, etc.

C. **IT Service**, (a sub-component of Information Technology) encompasses several main categories such as managed staffing, managed services, consultant arrangements, and cloud-based services, particularly whenever information is exchanged. In order to distinguish cloud-based services from data subscription, cloud-based services is a software distribution model in which applications are centrally hosted by independent software vendors (ISVs) or application service providers (ASPs) and made available to customers over a network, typically the Internet. Hosted services are a form of cloud-based services in which the vendor runs, manages, and modifies software on behalf of the client and manages the clients' data. Software as a Service (SaaS) is another form of cloud-based services in which applications provide the consumer the capability to use the provider's applications running on a cloud infrastructure. The provider manages all aspects of the application, including upgrades.

D. **Cyber System**: IT equipment or collections of IT equipment; any technology system (or collections thereof) capable of sending, receiving, or storing electronic data. Synonyms: GridIT, IT, information system, cyber asset, IT system. Examples: computing servers, user workstations, remote terminal units, phasor measurement units, network routers and switches, etc.

E. **Personally Identifiable Information (PII)**: The DOE CIO Guidance CS-38 directs it's organizations to use the Office of Management and Budget (OMB) definition for PII as "Any information about an individual maintained by an agency, including but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security numbers, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual."

5. Policy

Per DOE OCIO Guidance CS-38, and OMB Memoranda M-06-16, M-06-19, M-06-20, and DOE CIO Guidance CS-38A, PII data must be managed consistent with the following criteria:

1. All BPA-owned removable media, e.g. CDROMs, USB Drives, Flashdrives, Thumbdrives etc., containing PII must be encrypted with currently authorized encryption mechanisms;
2. All BPA-owned portable computers that contain PII must have an installed capability to encrypt PII;
3. All managers of BPA federal and contactor employees with authorized access to BPA-owned portable computers containing PII must direct their staff to use this encryption capability;
4. All managers of BPA federal and contractor employees using BPA-owned portable computers and/or media containing PII must revisit their staff's need for PII data every 90 days and require deletion of any file containing PII data determined to be no longer needed;
5. Remote access to PII requires two-factor authentication in accordance with authorized mechanisms, with an inactivity timeout per current policy;
6. All BPA federal and contractor employees must report all incidents involving the loss or theft of PII data within forty-five (45) minutes by calling the Cyber Security on-call emergency number, 503-230-5088, with a follow-up E-mail to the Cyber Security mailbox.
7. Cyber Security shall notify DOE Cyber Incident Advisory Capability (CIAC) within forty-five (45) minutes of discovering the incident.

6. Policy Exceptions

There are no exceptions to this policy.

7. Responsibilities

A. BPA Chief Information Officer (CIO)

Sponsors and owns this policy, overseeing periodic review of the policy, consistent with BPA strategic and operational plans and all statutory, regulatory, administrative, and OMB requirements. Reports any critical violations of this policy, or the standards and operations procedures referenced in this policy, to the BPA Executive Governance Body.

B. BPA Staff

Report all incidents involving the loss or theft of PII data within forty-five (45) minutes by calling the Cyber Security on-call emergency number, 503-230-5088, with a follow-up E-mail to the Cyber Security mailbox.

C. Cyber Security Staff

Notify DOE Cyber Incident Advisory Capability (CIAC) within forty-five (45) minutes of discovering an incident.

8. Standards & Procedures

Applicable standards and procedures for reporting PII incidents are published on the Cyber Security SharePoint Site.

9. Performance & Monitoring

On a regular basis a delegate of the OCIO shall conduct a review to identify and locate PII as defined by OMB. Any exceptions to this policy or critical violations shall be reported to the BPA Executive Governance Body.

10. Authorities & References

A. DOE O 200.1A, Information Technology Management

B. Clinger-Cohen Act of 1996

C. BPA Policy 473-2 Information Technology Policies

C. 40 U.S. Code SUBTITLE III: INFORMATION TECHNOLOGY MANAGEMENT

D. DOE OCIO Guidance CS-38 and CS-38A

E. OMB Memoranda M-06-16, M-06-19, and M-06-20

11. Review

This policy shall be reviewed by the policy owner at least every five years for relevant purpose, content, currency, effectiveness, and metrics.

12. Revision History

Version	Issue Date	Description of Change
1	3/25/2015	Initial creation by Mike Harris from Cyber Security BPA-20060809-0001 doc.
2	5/4/2016	Updates to definitions for consistency across policies, by Mike Harris.