PLATINUM
BUSINESS SERVICES, LLC

Safeguarding the Privacy of Personally Identifiable Information (PII)

Platinum Business Services, LLC

Jody Venkatesan, CISA, CISM, CGEIT, CRISC, CDPSE
President & CEO

Email: jvenkatesan@weareplatinum.net
Phone: 301-651-1297
Fax: 301-483-0104
Website: weareplatinum.net

4SBA Certified 8(a) HUBZone, Service-Disabled Veteran Owned Small Business (SDVOSB), Veteran-Owned Small Business (VOSB), Small Business (SB), Small Disadvantaged Business (SDB)
4TIN/EIN: 26-3462811
4Cage Code: 59N47
4DUNS: 828491410
4UEI: PCNMDK3FLJB9
4CIOSP3 NIH CIOSP3 SDVO
(Contract #HHSN316201800030W)
4GSA MAS Professional Services #GS00F344CA
4GSA MAS IT #GS-35F-0067Y
4GSA 8(a) STARS 3 #47QTCB21D0108

Safeguarding the Privacy of Personally Identifiable Information (PII)

Introduction

With the creation of the Internet forty years ago, when ARPANET converted to the TCP/IP protocol, the world of computing and communications changed dramatically. In the remarkably short span of just five years, the network's vulnerability was exposed with the unleashing of the Morris Worm. This malicious software inflicted substantial damage on a notable portion of the computers linked to the internet during that period.

The risks associated with the disclosure of personal information were obvious. Congress had already realized that the new technology offered the possibility of illegal activities, and in 1986, they passed the Computer Fraud and Abuse Act, legislation that was used to charge Robert Tappan Morris with a felony for the release of his worm. By 1996, Congress passed the Health Insurance Portability and Accountability Act (HIPAA) to specifically protect the personally identifiable information (PII) of all people related to their medical records. This legislation was followed by the Gramm-Leach-Bliley Act of 1999, which protects personal financial information. The Children's Online Privacy Protection Action was passed in 2000. These pieces of legislation augmented and expanded the fundamental standards established by the Privacy Act of 1974, which seeks to "balance the government's need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of privacy" {Introduction, Privacy Act of 1974.} Protecting the sanctity of individual information – specifically of Personally Identifiable Information (PII) – from illegal access by both internal and external entities continues to be a challenge for all government, financial, and healthcare institutions, both public and private.

Over the years, the tools used to manage this data while protecting it from inappropriate internal use and the technologies used by malevolent intruders to unlawfully access this information have become increasingly sophisticated. In fact, technologies keep advancing at an astounding rate, making keeping up with the "bad guys" a challenge for every security officer worldwide. The problem is a global issue, as intentional attacks by foreign governments or their representatives have superseded the risks offered by clever students like Morris. For example, the Office of Personnel Management was hacked in December 2014, with China allegedly stealing the personal information of approximately 4 million US citizens. Since then, the most threatening invasions of privacy have been more commonly associated with foreign nations – especially Russia and China – with massive and very sophisticated hacks like the SolarWinds trojan in 2020 and the Microsoft Server Side Request Forgery in 2021.

Safeguarding the Privacy of Personally Identifiable Information (PII)

So, what do we do, and how do we do it to protect the security of our nation's citizens and their PII?

There are a number of Government regulations and frameworks that guide agencies in selecting, implementing, and monitoring PII controls. Platinum's Security and Privacy Management experience includes using all these guidelines to provide a comprehensive approach to PII security. We use:

- FIPS 199 and NIST SP 800-60 to categorize information systems;
- FIP 200 & NIST SP 800-53 Rev. 5 to select Security Controls;
- NIST SP 800-70 to Implement Security Controls;
- NIST SP 800-53 Rev. 5 to Assess Security Controls;
- NIST SP 800-37 Rev. 2 to conduct IT Security Assessment and Authorization and obtain the Authorization to Operate;
- NIST SP 800-37 Rev. 2, NIST SP 800-53 Rev. 5, and NIST SP 800-53A Rev 5 to monitor Security Controls (Continuous Monitoring).

The critical functional activities surrounding effective Personally Identifiable Information Processing and Transparency are now encompassed in the NIST SP 800-53 Rev. 5 as a unique family of controls, which consolidated controls from previous versions and added specific PII controls. While previous versions addressed PII as a subset of other control families, it is now its specific set of controls to be implemented and evaluated. As this is the most comprehensive look at PII controls, effectively spanning all other applicable controls, NIST SP 800-53A Rev 5 is where we start.

We begin by evaluating the policies and procedures that govern privacy-related processes. We note that this is strongly linked to the implementation of Zero Trust Architecture (ZTA), specifically as it addresses access controls and permissions. We will work with our clients to develop a clearly defined set of policies based on all applicable laws and regulations, which may be defined in a privacy plan, privacy program plan, or privacy policy linked to the organization's ZTA and the access controls policies and procedures. The policy(ies) will identify:

- Personnel or role-based personnel to be informed of and trained in the policies.
- The organizational level at which the privacy controls are assigned, such as mission or business process level, or system level; again, this is linked to the access controls, particularly in a role-based approach to applying for controls and permissions.
- The individual or position responsible for managing privacy/PII information processing.
- The frequency with which the policy is reviewed and potentially updated, including the impact of new regulations or recommendations from NIST or other security agencies.
- The frequency and/or triggers that result in the PII processes being reviewed and updated as needed.
- Define the relationships and coordination among the various sectors of the organization that have some impact on the management of PII.

Safeguarding the Privacy of Personally Identifiable Information (PII)

Once a policy has been established, we will work with our clients to define the authority and processes used to use and manage PII. This will include the allowable uses of PII, restrictions on the types of PII used, the authority that allows the PII to be used, how PII is data tagged, and how the use of PII is enforced, both by manual and automated processes. The fields within a database containing PII will be identified and tagged, including Social Security numbers and other information protected under First Amendment rights and the Privacy Act. Taken together, these steps address the range of information to be protected, which we do by meticulously categorizing and labeling the PII elements, reinforcing measures to uphold privacy regulations and safeguarding sensitive data.

A process for interacting with the Change Control Board (CCB) is essential for the effective management and protection of PII. Whenever a change authorization is required of the CCB, a thorough review must be conducted to determine if the change will impact PII use or controls. Adequate protective measures should be taken to ensure appropriate measures are in place before the CCB approves the change.

We establish robust mechanisms for both automated and manual processes to ensure the accurate tracking of PII processing purposes. Regular audits, verification, and validation are crucial to ensuring the ongoing protection of this critical data. This includes ensuring that individuals have given consent to use their data and what limitations are imposed on that consent so that permissions can be tailored appropriately to the individual's wishes. This also includes recording the presentation of the Privacy Act information to the individual and providing a mechanism for the individual to change the terms of their consent if desired. The individual should also be advised how the information is maintained in a records system.

The care and protection of PII may not be exceptionally complex, but it demands careful attention to detail and effective integration within any enterprise's overall cybersecurity and configuration management framework. Platinum is experienced in meeting these requirements and implementing a fully compliant system, adhering to all applicable legislation and regulations. We are committed to assisting you in safeguarding some of the most sensitive information within your systems.