



**WIDEPOINT PERSONAL IDENTITY VERIFICATION  
SHARED SERVICE PROVIDER PROGRAM  
(WIDEPOINT PIV SSP)**

*PRIVACY IMPACT ASSESSMENT*

**WIDEPOINT PIV SSP PIA**

**Version 2.4**

**January 21, 2021**

WidePoint Cybersecurity Solutions Corporation  
11250 Waples Mill Road  
South Tower, Suite 210  
Fairfax, VA 22030

---

♥ Copyright 2021, WidePoint Cybersecurity Solutions Corporation  
All Rights Reserved

*This document is proprietary and may not be disclosed to other parties, be it pursuant to the  
Freedom of Information Act or to any other law or regulation.*

---

**Notice:** Operational Research Consultants, Inc. (ORC), a wholly-owned subsidiary of WidePoint Corporation, has changed its legal name to WidePoint Cybersecurity Solutions Corporation, hereafter referred to simply as WidePoint. This is a legal name change only for branding purposes with no change to ownership, corporation type or other status. Any and all references to "WidePoint" within this document refers specifically and only to WidePoint Cybersecurity Solutions Corporation, the wholly-owned subsidiary of WidePoint Corporation, and not to WidePoint Corporation as a whole. Any reference or citing of personnel within this document, such as "WidePoint CEO", refers to the CEO of WidePoint Cybersecurity Solutions Corporation and not the CEO of WidePoint Corporation.

---

## STAKEHOLDERS

Name of Information System Security Manager (ISSM):

- Arpan patel

Name of Program Manager/System Owner:

- Cheryl Jenkins

## SIGNATURE PAGE

Signed:

DocuSigned by:

*Arpan Patel*

8B059AABDAF1477...

---

Information System Security Manager (ISSM)

DocuSigned by:

*Cheryl Jenkins*

33B71CFAE732436...

---

Program Manager/System Owner

DocuSigned by:

*Richard Speidel*

174D5411183F48A...

---

Chief Privacy Officer (CPO) - Under the direction of the Senior Agency Official for Privacy (SAOP), the CPO is responsible for evaluating the PIA and ensuring the program manager/system owner has provided complete privacy-related information.

---

**DOCUMENT REVISION HISTORY**

<b>Date</b>	<b>Comments</b>	<b>Version</b>	<b>Author</b>
2017-04-12	Initial Version	1.0	Michael Boorum
2018-01-13	Updated to follow new format	2.0	Richard Webb
2019-10-17	Annual review and update	2.1	Richard Webb
2020-03-27	Updates and responses to GSA Privacy officials' comments	2.2	Richard Webb
2020-03-30	Added Signature Page	2.3	Qamar Hasan (Privacy Office)
2021-01-21	Annual review and update	2.4	Richard Webb

**POINT of CONTACT**

Richard Speidel

[gsa.privacyact@gsa.gov](mailto:gsa.privacyact@gsa.gov)**Chief Privacy Officer  
GSA IT  
1800 F Street NW  
Washington, DC 20405**

---

♥ Copyright 2021, WidePoint Cybersecurity Solutions Corporation  
All Rights Reserved

*This document is proprietary and may not be disclosed to other parties, be it pursuant to the  
Freedom of Information Act or to any other law or regulation.*

---

## TABLE OF CONTENTS

1	SECTION 1.0 PURPOSE OF COLLECTION.....	7
1.1	WHY IS WIDEPOINT COLLECTING THE INFORMATION? .....	7
1.2	WHAT LEGAL AUTHORITY AND/OR AGREEMENTS ALLOW WIDEPOINT TO COLLECT THE INFORMATION? .....	7
1.3	IS THE INFORMATION SEARCHABLE BY A PERSONAL IDENTIFIER, FOR EXAMPLE A NAME OR SOCIAL SECURITY NUMBER? IF SO, WHAT SYSTEM OF RECORDS NOTICE(S) APPLY/APPLIES TO THE INFORMATION BEING COLLECTED? .....	8
1.4	HAS ANY INFORMATION COLLECTION REQUEST (ICR) BEEN SUBMITTED TO OR APPROVED BY THE OFFICE OF MANAGEMENT AND BUDGET (OMB)? IF YES, PROVIDE THE RELEVANT NAMES, OMB CONTROL NUMBERS, AND EXPIRATION DATES.....	8
1.5	HAS A RECORDS RETENTION SCHEDULE BEEN APPROVED BY THE NATIONAL ARCHIVES AND RECORDS ADMINISTRATION (NARA)? EXPLAIN HOW LONG AND FOR WHAT REASON THE INFORMATION IS RETAINED. ....	8
1.6	ARE THERE ANY PRIVACY RISKS THAT RELATE TO THE PURPOSE OF THE COLLECTION? IF SO, HOW WILL GSA MITIGATE THESE RISKS?.....	8
2	SECTION 2.0 OPENNESS AND TRANSPARENCY .....	9
2.1	WILL INDIVIDUALS BE GIVEN NOTICE PRIOR TO THE COLLECTION AND/OR SHARING OF PERSONAL INFORMATION ABOUT THEMSELVES? IF NOT, PLEASE EXPLAIN.....	9
2.2	ARE THERE ANY PRIVACY RISKS FOR THIS SYSTEM THAT RELATE TO OPENNESS AND TRANSPARENCY? IF SO, HOW WILL GSA MITIGATE THESE RISKS? .....	9
3	SECTION 3.0 DATA MINIMIZATION.....	10
3.1	WHOSE INFORMATION IS INCLUDED IN THE SYSTEM, APPLICATION OR PROJECT?.	10
3.2	WHAT PII WILL THE SYSTEM, APPLICATION OR PROJECT INCLUDE? .....	10
3.3	WHY IS THE COLLECTION AND USE OF THE PII NECESSARY TO THE SYSTEM, APPLICATION OR PROJECT? .....	10
3.4	WILL THE SYSTEM, APPLICATION OR PROJECT CREATE OR AGGREGATE NEW DATA ABOUT THE INDIVIDUAL? IF SO, HOW WILL THIS DATA BE MAINTAINED AND USED? .....	10
3.5	WHAT PROTECTIONS EXIST TO PROTECT THE CONSOLIDATED DATA AND PREVENT UNAUTHORIZED ACCESS? .....	11
3.6	WILL THE SYSTEM MONITOR THE PUBLIC, GSA EMPLOYEES OR CONTRACTORS?.	12
3.7	WHAT KINDS OF REPORT(S) CAN BE PRODUCED ON INDIVIDUALS? .....	12
3.8	WILL THE DATA INCLUDED IN ANY REPORT(S) BE DE-IDENTIFIED? IF SO, WHAT PROCESS(ES) WILL BE USED TO AGGREGATE OR DE-IDENTIFY THE DATA? .....	12
3.9	ARE THERE ANY PRIVACY RISKS FOR THIS SYSTEM THAT RELATE TO DATA MINIMIZATION? IF SO, HOW WILL GSA MITIGATE THESE RISKS?.....	12
4	SECTION 4.0 LIMITS ON USES AND SHARING OF INFORMATION .....	13
4.1	IS THE INFORMATION IN THE SYSTEM, APPLICATION OR PROJECT LIMITED TO ONLY THE INFORMATION THAT IS NEEDED TO CARRY OUT THE PURPOSE OF THE COLLECTION?13	
4.2	WILL GSA SHARE ANY OF THE INFORMATION WITH OTHER INDIVIDUALS, FEDERAL AND/OR STATE AGENCIES, OR PRIVATE SECTOR ORGANIZATIONS? IF SO, HOW WILL GSA SHARE THE INFORMATION? .....	13
4.3	IS THE INFORMATION COLLECTED DIRECTLY FROM THE INDIVIDUAL OR IS IT TAKEN FROM ANOTHER SOURCE? IF SO, WHAT IS THE OTHER SOURCE(S)? .....	13

---

4.4	WILL THE SYSTEM, APPLICATION OR PROJECT INTERACT WITH OTHER SYSTEMS, APPLICATIONS OR PROJECTS, EITHER WITHIN OR OUTSIDE OF GSA? IF SO, WHO, HOW AND IS A FORMAL AGREEMENT(S) IN PLACE? .....	13
4.5	ARE THERE ANY PRIVACY RISKS FOR THIS SYSTEM, APPLICATION OR PROJECT THAT RELATE TO USE LIMITATION? IF SO, HOW WILL GSA MITIGATE THESE RISKS? .....	13
5	SECTION 5.0 DATA QUALITY AND INTEGRITY .....	14
5.1	HOW WILL THE INFORMATION COLLECTED BE VERIFIED FOR ACCURACY AND COMPLETENESS? .....	14
5.2	ARE THERE ANY PRIVACY RISKS FOR INDIVIDUALS WHOSE INFORMATION IS COLLECTED OR USED THAT RELATE TO DATA QUALITY AND INTEGRITY? IF SO, HOW WILL GSA MITIGATE THESE RISKS?.....	14
6	SECTION 6.0 SECURITY .....	15
6.1	WHO OR WHAT WILL HAVE ACCESS TO THE DATA IN THE SYSTEM, APPLICATION OR PROJECT? WHAT IS THE AUTHORIZATION PROCESS TO GAIN ACCESS?.....	15
6.2	HAS WIDEPOINT COMPLETED A SYSTEM SECURITY PLAN FOR THE INFORMATION SYSTEM(S) OR APPLICATION? .....	15
6.3	HOW WILL THE SYSTEM OR APPLICATION BE SECURED FROM A PHYSICAL, TECHNOLOGICAL, AND MANAGERIAL PERSPECTIVE? .....	15
6.4	ARE THERE MECHANISMS IN PLACE TO IDENTIFY SUSPECTED OR CONFIRMED SECURITY INCIDENTS AND BREACHES OF PII? IF SO, WHAT ARE THEY?.....	16
6.5	ARE THERE ANY PRIVACY RISKS FOR THIS SYSTEM, APPLICATION OR PROJECT THAT RELATE TO SECURITY? IF SO, HOW WILL THE WIDEPOINT PIV SSP MITIGATE THESE RISKS?16	
7	SECTION 7.0 INDIVIDUAL PARTICIPATION .....	17
7.1	WHAT OPPORTUNITIES ARE AVAILABLE FOR INDIVIDUALS TO CONSENT TO USES, DECLINE TO PROVIDE INFORMATION OR OPT OUT OF PROVIDING INFORMATION? IF NO OPPORTUNITIES EXIST TO CONSENT, DECLINE OR OPT OUT, PLEASE EXPLAIN. ....	17
7.2	WHAT PROCEDURES ALLOW INDIVIDUALS TO ACCESS THEIR INFORMATION?.....	17
7.3	CAN INDIVIDUALS AMEND INFORMATION ABOUT THEMSELVES? IF SO, HOW?.....	18
7.4	ARE THERE ANY PRIVACY RISKS FOR THIS SYSTEM, APPLICATION OR PROJECT THAT RELATE TO INDIVIDUAL PARTICIPATION? IF SO, HOW WILL THE WIDEPOINT PIV SSP MITIGATE THESE RISKS?.....	18
8	SECTION 8.0 AWARENESS AND TRAINING.....	19
8.1	DESCRIBE WHAT PRIVACY TRAINING IS PROVIDED TO USERS, EITHER GENERALLY OR SPECIFICALLY RELEVANT TO THE SYSTEM, APPLICATION OR PROJECT. ....	19
8.2	ARE THERE ANY PRIVACY RISKS FOR THIS SYSTEM, APPLICATION OR PROJECT THAT RELATE TO AWARENESS AND TRAINING? IF SO, HOW WILL GSA MITIGATE THESE RISKS?..	19
9	SECTION 9.0 ACCOUNTABILITY AND AUDITING.....	20
9.1	HOW DOES THE SYSTEM, APPLICATION OR PROJECT ENSURE THAT THE INFORMATION IS USED IN ACCORDANCE WITH THE STATED PRACTICES IN THIS PIA? .....	20
9.2	ARE THERE ANY PRIVACY RISKS FOR THIS SYSTEM, APPLICATION OR PROJECT THAT RELATE TO ACCOUNTABILITY AND AUDITING? IF SO, HOW WILL GSA MITIGATE THESE RISKS? .....	20
10	APPENDIX A .....	21
11	APPENDIX B .....	22

---

## 1 SECTION 1.0 PURPOSE OF COLLECTION

### 1.1 WHY IS WIDEPOINT COLLECTING THE INFORMATION?

WidePoint operates as a Federal Personal Identity Verification (PIV) Shared Service Provider, hereafter referred to as “The WidePoint PIV SSP”, for federal agencies to issue PIV credentials and digital certificates that identify individuals and devices for use with electronic authorizations such as digital signing, smart card logon to networks, access to websites and applications as well as physical access authorizations. The WidePoint PIV SSP operates a certification authority infrastructure that issues digital certificates contained on HSPD-12 PIV credentials issued to federal agencies and their contractors. Additionally, the WidePoint PIV SSP manages the life cycle of those issued credentials and certificates to include revocation, renewal, and expiration. In order to issue digital certificates and PIV credentials that identify a human or a device digitally, identification information is collected to ensure that human or device that the certificate or credential represents is who they say they are. The WidePoint PIV SSP digital certificate credentials are utilized to provide secure authentication and trusted transactions for federal employees and contractors, and their devices (including web services and domain authentication). These credentials can be used to:

- authenticate to government and organization websites
- contract for the purchase of goods or services
- verify the identity of electronic mail correspondents
- verify the identity of web/application servers and devices
- verify the identity of individuals and devices accessing data servers
- verify the identity of individuals for physical access

### 1.2 WHAT LEGAL AUTHORITY AND/OR AGREEMENTS ALLOW WIDEPOINT TO COLLECT THE INFORMATION?

The WidePoint PIV SSP is approved by the Federal PKI Policy Authority to issue certificates under the Federal PKI Common Policy Framework, hereafter referred to as “FPCPF” see here - <https://www.idmanagement.gov/topics/fpki/#certificate-policies>. The WidePoint PIV SSP has been an approved provider of credentials under the FPCPF since 2007. WidePoint’s most recent Memorandum of Agreement (MOA) with the Federal PKI Policy Authority can be found in APPENDIX A.

---

**1.3 IS THE INFORMATION SEARCHABLE BY A PERSONAL IDENTIFIER, FOR EXAMPLE A NAME OR SOCIAL SECURITY NUMBER? IF SO, WHAT SYSTEM OF RECORDS NOTICE(S) APPLY/APPLIES TO THE INFORMATION BEING COLLECTED?**

In accordance with Federal Information Processing Standard 201-2 Personal Identity Verification (PIV) of Federal Employees and Contractors published August 2013, hereafter referred to as "FIPS 201-2", the WidePoint PIV SSP does collect information that is personally identifiable in order to issue a PIV credential to a Federal Employee or a Contractor. The types of Personally Identifiable Information, hereafter referred to as "PII", is detailed by Section 2 of FIPS 201-2, in particular Section 2.4 – Biometric Data Collection for PIV Card, and Section 2.6 – Chain of Trust which describes the data captured to tie an individual to the biometric data captured as described in Section 2.4.

Individual agencies are responsible for creating their own System of Records Notice(s), hereafter referred to as "SORNs".

**1.4 HAS ANY INFORMATION COLLECTION REQUEST (ICR) BEEN SUBMITTED TO OR APPROVED BY THE OFFICE OF MANAGEMENT AND BUDGET (OMB)? IF YES, PROVIDE THE RELEVANT NAMES, OMB CONTROL NUMBERS, AND EXPIRATION DATES.**

No.

**1.5 HAS A RECORDS RETENTION SCHEDULE BEEN APPROVED BY THE NATIONAL ARCHIVES AND RECORDS ADMINISTRATION (NARA)? EXPLAIN HOW LONG AND FOR WHAT REASON THE INFORMATION IS RETAINED.**

In accordance with FPCPF Section 5.5 – Records Archival and Section 5.5.2 - Retention Period for Archive and the WidePoint PIV SSP Certification Practice Statement Section 5.5 – Records Archival and Section 5.5.2 - Retention Period for Archive, the WidePoint PIV SSP maintains collected information for 10 years and 6 months in accordance with retention requirements specified for medium levels of assurance. The WidePoint PIV SSP does not currently issue high level of assurance. In the event that the WidePoint PIV SSP is approved to issue high level of assurance credentials, the retention period would extend to 20 years in accordance with FPCPF Section 5.5.

**1.6 ARE THERE ANY PRIVACY RISKS THAT RELATE TO THE PURPOSE OF THE COLLECTION? IF SO, HOW WILL GSA MITIGATE THESE RISKS?**

**Privacy Risk:** User information may be exposed during the request process.

**Mitigation:** Request processes are performed under Secure SSL sessions by an FIPS 201 approved Card Management System and the WidePoint PIV SSP Certificate Authority. These instances are protected by SSL certificates that are issued in accordance with the WidePoint PIV SSP Certificate Practice S and the FPCPF.

---

## 2 SECTION 2.0 OPENNESS AND TRANSPARENCY

### 2.1 WILL INDIVIDUALS BE GIVEN NOTICE PRIOR TO THE COLLECTION AND/OR SHARING OF PERSONAL INFORMATION ABOUT THEMSELVES? IF NOT, PLEASE EXPLAIN.

The FPCPF Certificate Policy Section 9.4 – Privacy of Personal Information and subsections along with the WidePoint PIV SSP CPS Section 9.4 – Privacy of Personal Information and subsections provide public notice of what data is collected, what data is treated as private and what data is deemed not private, and how that data is to be protected. Additional notices are determined by the federal department/agency that is sponsoring the individual for a PIV Card.

### 2.2 ARE THERE ANY PRIVACY RISKS FOR THIS SYSTEM THAT RELATE TO OPENNESS AND TRANSPARENCY? IF SO, HOW WILL GSA MITIGATE THESE RISKS?

No. WidePoint's Privacy Act Notice is posted on all WidePoint sites (Web and physical) and describes WidePoint's actions with respect to PII. As part of the application process for any WidePoint credential, a prospective Subscriber must agree to a set of obligations which include acknowledgement of WidePoint's Privacy Act Notice.

### **3 SECTION 3.0 DATA MINIMIZATION**

#### **3.1 WHOSE INFORMATION IS INCLUDED IN THE SYSTEM, APPLICATION OR PROJECT?**

Employees and contractors requiring PIV credentials for federal agencies.

#### **3.2 WHAT PII WILL THE SYSTEM, APPLICATION OR PROJECT INCLUDE?**

In accordance with Federal Information Processing Standard 201-2 Personal Identity Verification (PIV) of Federal Employees and Contractors published August 2013, hereafter referred to as "FIPS 201-2", the WidePoint PIV SSP does collect information that is personally identifiable in order to issue a PIV credential to a Federal Employee or a Contractor. The types of PII is detailed by Section 2 of FIPS 201-2, in particular Section 2.4 – Biometric Data Collection for PIV Card, and Section 2.6 – Chain of Trust which describes the data captured to tie an individual to the biometric data captured as described in Section 2.4.

As such, the WidePoint PIV SSP collects name, date of birth, email address, photograph, and fingerprint minutiae. SSN is used for individuals who choose (optional) to provide it for identity-proofing purposes. Other identity source documents are available as alternatives. As a general rule, the WidePoint PIV SSP does not collect Social Security Numbers. If it is collected as a form of identification, the SSN is stored as the document name for the document presented for identification purposes.

#### **3.3 WHY IS THE COLLECTION AND USE OF THE PII NECESSARY TO THE SYSTEM, APPLICATION OR PROJECT?**

In accordance with Federal Information Processing Standard 201-2 Personal Identity Verification (PIV) of Federal Employees and Contractors, hereafter referred to as "FIPS 201-2", the WidePoint PIV SSP does collect information that is personally identifiable in order to issue a PIV credential to a Federal Employee or a Contractor. Types of PII data is detailed in Section 2 of FIPS 201-2, in particular Section 2.4 – Biometric Data Collection for PIV Card, and Section 2.6 – Chain of Trust which describes the data captured to tie an individual to the biometric data captured as described in Section 2.4.

#### **3.4 WILL THE SYSTEM, APPLICATION OR PROJECT CREATE OR AGGREGATE NEW DATA ABOUT THE INDIVIDUAL? IF SO, HOW WILL THIS DATA BE MAINTAINED AND USED?**

Yes. The WidePoint PIV SSP collects PII information as defined in Section 3.3 of this document and ties that information to digital certificates that are issued to PIV credentials so that PIV Credential holders may assert their identity electronically. Only Name, email address and affiliation are tied to the certificate (not SSN).

---

### 3.5 WHAT PROTECTIONS EXIST TO PROTECT THE CONSOLIDATED DATA AND PREVENT UNAUTHORIZED ACCESS?

The WidePoint PIV SSP systems that collect PII data and issue digital certificates in accordance with the FPCPF are certified by the General Services Administration (GSA) up to FISMA-Moderate. The latest FISMA-Moderate ATO can be found in APPENDIX B of this document.

In order to protect data and prevent unauthorized access, roles are defined within the WidePoint PIV SSP CPS in Section 5.2.1 – Trusted Roles. There are 4 trusted roles:

- **Administrator** – The WidePoint PIV SSP refers to the Administrator role as the WidePoint Certificate Authority Administrator. This role is responsible for installation, configuration and operation of the WidePoint PIV SSP Certificate Authorities and Certificate Status Authorities.
- **Officer** – The WidePoint PIV SSP refers to the Officer role as the WidePoint Registration Authority. This role is responsible for issuing and revoking certificates/credentials. The role may have further sub classification in terms of the issuance of PIV credentials (i.e., Registrar and Issuer).
- **Auditor** - The Corporate Security Auditor is responsible for backing up and archiving all audit data and reviewing the audit logs recorded by WidePoint PIV SSP Certificate Authorities, Card Management Systems, Registration Authority Workstations, and Certificate Status Servers.
- **Operator** - The WidePoint PIV SSP refers to the Operator as the WidePoint System Administrator. This role is primarily responsible for administration of WidePoint PIV SSP Certificate Authorities, Card Management Systems, Registration Authority Workstations, and Certificate Status Servers host computers and operating systems to include initial configuration, account management, network configuration and system backup and recovery among other things.

Privacy data is protected at several levels. With respect to the application and the machine running those applications, two party control is implemented. WidePoint Certificate Authority Administrators are responsible for the application that hosts the PII data – i.e. WidePoint PIV SSP Certificate Authorities, Card Management Systems, Registration Authority Workstations, and Certificate Status Servers. WidePoint System Administrators are responsible for the machine that hosts these applications. The applications and machines are physically hosted within the WidePoint Secure Network Operations Center (SNOC) in a cage that requires one WidePoint Certificate Authority Administrator and one WidePoint System Administrator in order to access the cage hosting the systems. Additionally, WidePoint System Administrators have root access privileges to the systems but do not have the ability to operate the applications. WidePoint System Administrators must grant WidePoint Certificate Authority Administrators root privileges in order for the WidePoint Certificate Authority Administrators to administer the applications of CMS, CA or CSS. All work is done under two party control.

With respect to the process of issuing PIV credentials to individual subscribers, the WidePoint Registrar role is responsible for gathering user information and vetting that information before

---

passing that information onto the Issuer role who is responsible for the issuance of the PIV credential to the user. Issuance of a PIV credential requires both a WidePoint Registrar and WidePoint Issuer to complete. No person may act as both a WidePoint Registrar and WidePoint Issuer for the issuance of a particular PIV credential. WidePoint Registrar and WidePoint Issuers must authenticate under a secure session using their individual PIV credential to the WidePoint PIV SSP Card Management System (WidePoint PIV SSP CPS) in order perform their duties with respect to PIV credential issuance. User privacy data is restricted to authenticated access by either the WidePoint Registrar or WidePoint Issuer.

### **3.6 WILL THE SYSTEM MONITOR THE PUBLIC, GSA EMPLOYEES OR CONTRACTORS?**

No. Performance monitoring is at the operating system level. Since this is not a system that does continuous monitoring of the credentials that it issues or performs periodic re-vetting of individuals who already have credentials..

### **3.7 WHAT KINDS OF REPORT(S) CAN BE PRODUCED ON INDIVIDUALS?**

Monthly reports of active PIV Credentials that show user name, email address, issuance date and expiration date, employee or contractor status are generated and submitted to customer departments/agencies. Reports are encrypted and provided to the departments/agencies through a secure portal that requires access by a designated Point of Contact within the department/agency. Only the designated Point of Contact can download the report.

### **3.8 WILL THE DATA INCLUDED IN ANY REPORT(S) BE DE-IDENTIFIED? IF SO, WHAT PROCESS(ES) WILL BE USED TO AGGREGATE OR DE-IDENTIFY THE DATA?**

No.

### **3.9 ARE THERE ANY PRIVACY RISKS FOR THIS SYSTEM THAT RELATE TO DATA MINIMIZATION? IF SO, HOW WILL GSA MITIGATE THESE RISKS?**

N/A.

---

## 4 SECTION 4.0 LIMITS ON USES AND SHARING OF INFORMATION

### 4.1 IS THE INFORMATION IN THE SYSTEM, APPLICATION OR PROJECT LIMITED TO ONLY THE INFORMATION THAT IS NEEDED TO CARRY OUT THE PURPOSE OF THE COLLECTION?

Yes, PII collected by the WidePoint PIV SSP is limited to the information required by FIPS 201-2, the FPCPF Certificate Policy, and the WidePoint PIV SSP CPS.

### 4.2 WILL GSA SHARE ANY OF THE INFORMATION WITH OTHER INDIVIDUALS, FEDERAL AND/OR STATE AGENCIES, OR PRIVATE SECTOR ORGANIZATIONS? IF SO, HOW WILL GSA SHARE THE INFORMATION?

PII information collected by the WidePoint PIV SSP is not shared with other individuals, Federal and/or state agencies, except those departments/agencies who are subscribers to the WidePoint PIV SSP for issuance of PIV credentials to their federal employees or contractors. Individuals may view their own PII data and, as stipulated in section 4.1.1 – Who can submit a Key Recovery Application of the FPKI Key Recovery Policy (see here - <https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/fpki-krp-v1.0-10-6-2017.pdf>), authorized third-party requestors (e.g. law enforcement personnel) with a court order from a competent court.

### 4.3 IS THE INFORMATION COLLECTED DIRECTLY FROM THE INDIVIDUAL OR IS IT TAKEN FROM ANOTHER SOURCE? IF SO, WHAT IS THE OTHER SOURCE(S)?

Biometric PII information – including fingerprints, eye and hair color, and height - is collected directly from the user during an in-person enrollment process as described in FIPS 201-2, FPCPF, and the WidePoint PIV SSP CPS. PII information of non-biometric data may be directly uploaded by the department/agency for which the individual is a federal employee or contractor.

### 4.4 WILL THE SYSTEM, APPLICATION OR PROJECT INTERACT WITH OTHER SYSTEMS, APPLICATIONS OR PROJECTS, EITHER WITHIN OR OUTSIDE OF GSA? IF SO, WHO, HOW AND IS A FORMAL AGREEMENT(S) IN PLACE?

No. The WidePoint PIV SSP does not share data with any other systems. The WidePoint PIV SSP has no interconnection agreements. Data may only be shared as previously stipulated and in accordance with the governing documents: FIPS 201-2, FPCPF Certificate Policy, the FPKI Key Recovery Policy and the WidePoint PIV SSP CPS.

### 4.5 ARE THERE ANY PRIVACY RISKS FOR THIS SYSTEM, APPLICATION OR PROJECT THAT RELATE TO USE LIMITATION? IF SO, HOW WILL GSA MITIGATE THESE RISKS?

N/A.

---

## 5 SECTION 5.0 DATA QUALITY AND INTEGRITY

### 5.1 HOW WILL THE INFORMATION COLLECTED BE VERIFIED FOR ACCURACY AND COMPLETENESS?

PII data collected is verified against physical documentation that is used to establish the identity of the PIV credential recipient. The biometric capture devices use algorithms to determine if the capture is a good capture and repeatable in the case of fingerprint capture.

### 5.2 ARE THERE ANY PRIVACY RISKS FOR INDIVIDUALS WHOSE INFORMATION IS COLLECTED OR USED THAT RELATE TO DATA QUALITY AND INTEGRITY? IF SO, HOW WILL GSA MITIGATE THESE RISKS?

No. The biometric data captured during the enrollment process for a PIV Credential is in accordance with NIST Special Publication 800-76-2 Biometric Specifications for Personal Identity Verification.

---

## 6 SECTION 6.0 SECURITY

### 6.1 WHO OR WHAT WILL HAVE ACCESS TO THE DATA IN THE SYSTEM, APPLICATION OR PROJECT? WHAT IS THE AUTHORIZATION PROCESS TO GAIN ACCESS?

Employees of the the WidePoint PIV SSP who have access to PII contained within the WidePoint PIV SSP are in trusted roles assigned by the WidePoint Chief Security Officer and who have undergone role-based training as outlined in the WidePoint System Security Plan, Awareness and Training Control AT-3 – Role-Based Security Training. AT-3 Role-Based Training applies to WidePoint Certificate Authority Administrators who are responsible for the WidePoint PIV SSP applications, WidePoint System Administrators who are responsible for the WidePoint PIV SSP systems and operating systems, WidePoint Issuers who approve the issuance of the PIV Credential, and WidePoint Registrars who perform the vetting of the individual to receive the PIV Credential. These role assignments include review of all governing policy, practice and procedure documents.

Role Based users may have access to PII Data contained within the system as previously detailed in Section 3.5 of this document. For WidePoint Certificate Authority Administrators and WidePoint System Administrators that govern the operating system and the application respectively, risk is mitigated by having two-party control on all systems that contain PII data (i.e. one (1) WidePoint Certificate Authority Administrator and one (1) WidePoint System Administrator must authenticate to the system before any action can be accomplished). The WidePoint systems that collect PII data and issue digital certificates in accordance with the FPCPF are certified by the General Services Administration (GSA) up to FISMA-Moderate.

### 6.2 HAS WIDEPOINT COMPLETED A SYSTEM SECURITY PLAN FOR THE INFORMATION SYSTEM(S) OR APPLICATION?

Yes. The current version is 6.2.3.7 dated 20 December 2020.

### 6.3 HOW WILL THE SYSTEM OR APPLICATION BE SECURED FROM A PHYSICAL, TECHNOLOGICAL, AND MANAGERIAL PERSPECTIVE?

The WidePoint systems that collect PII data and issue digital certificates in accordance with the FPCPF are certified by the General Services Administration (GSA) up to FISMA-Moderate. The latest FISMA-Moderate ATO can be found in APPENDIX B of this document.

Physical and technological controls are defined in the WidePoint PIV SSP CPS Section 5 – Facility, Management, and Operational Controls and Section 6 – Technical Security Controls. These are further defined in the WidePoint System Security Plan through Control Family Physical and Environmental Protection – all controls, Control Family System and Services Acquisition Control, in particular SA-4: Acquisition Process, Control Family Personnel Security – all controls, Control Family Media Protection – all controls, Control Family Maintenance – all controls.

---

**6.4 ARE THERE MECHANISMS IN PLACE TO IDENTIFY SUSPECTED OR CONFIRMED SECURITY INCIDENTS AND BREACHES OF PII? IF SO, WHAT ARE THEY?**

The WidePoint PIV SSP is certified at FISMA-Moderate and is audited by a third party auditor. Systems are configured to provide audit logging capabilities in compliance with the WidePoint System Security Plan Audit and Accountability Control AU-2 – Type of events and collected to a Splunk system that is used to analyze operating system level logging. Systems are evaluated by Nessus and OWASP scans and internal POA&Ms in accordance with Security Assessment and Authorization Control CA-5- Plan of Action and Milestones are conducted to address any findings. Penetration tests are performed in accordance with Security Assessment and Authorization Control CA-8 Penetration Testing.

Additionally, WidePoint conducts annual exercises for incident responses and is detailed in the WidePoint PIV SSP Incident Response Plan. WidePoint has also developed and conducts exercises in incident response separate from contingency planning.

**6.5 ARE THERE ANY PRIVACY RISKS FOR THIS SYSTEM, APPLICATION OR PROJECT THAT RELATE TO SECURITY? IF SO, HOW WILL THE WIDEPOINT PIV SSP MITIGATE THESE RISKS?**

Yes. There is a possibility that reporting data involving incidents may involve PII data. Security reporting is scrubbed of PII data during the compilation. In addition, any audit data that is removed from the system is encrypted, password protected and placed on unalterable media (i.e. CDs/DVDs).

---

## 7 SECTION 7.0 INDIVIDUAL PARTICIPATION

### 7.1 WHAT OPPORTUNITIES ARE AVAILABLE FOR INDIVIDUALS TO CONSENT TO USES, DECLINE TO PROVIDE INFORMATION OR OPT OUT OF PROVIDING INFORMATION? IF NO OPPORTUNITIES EXIST TO CONSENT, DECLINE OR OPT OUT, PLEASE EXPLAIN.

In order for federal employees and contractors to obtain PIV credentials consistent with FIPS 201-2, Federal Employees and Contractors must present PII data as specified in Section 3.2 of this document. Federal employees and contractors who decline to provide information are not eligible to receive a PIV from the WidePoint PIV SSP. Additionally, PIV Card applicants are employees or contractors of federal departments or agencies, and are governed by the policies of their respective department or agency. PIV card applicants are advised by the WidePoint PIV SSP system of the Conditions of Use for their PIV card. These conditions are spelled out below:

- The PIV card is your identification for the Agency. The PIV card is the property of the department or agency, is issued by the department or agency to the cardholder only, and is non-transferable.
- Use of the PIV card may be revoked at the department or agency's request or by the WidePoint PIV SSP's sole discretion for violation of the department or agency's and or WidePoint PIV SSP's policies and procedures. Employees and contractors must relinquish the card upon separation from the department or agency. The department or agency must revoke the card and properly destroy.
- The PIV card must be presented upon request at the time of use to obtain access or to establish official Agency status. The PIV Card is to be used only by the person to whom it is issued. Only the cardholder can present the PIV Card for access and other privileges. The PIV Card will be confiscated, certificates revoked, and card destroyed if presented by someone other than the Cardholder.
- The department agency rules and regulations govern the use of the PIV card.

### 7.2 WHAT PROCEDURES ALLOW INDIVIDUALS TO ACCESS THEIR INFORMATION?

This is governed by the policies of the WidePoint PIV SSP department/agency customers.

Additionally, the WidePoint PIV SSP Digital Identity Acceptance Statement under Identification and Authentication Control IA-1: Identification and Authentication Policy and Procedures defines the respective Assurance Levels of the WidePoint PIV SSP.

The Identity Assurance Level for the WidePoint PIV SSP is IAL3 as the PIV Credential issuance process requires physical presence for identity proofing.

---

The Authentication Assurance Level for the WidePoint PIV SSP is AAL2 as the PIV Credential issued through this process is a multi-factor authentication vehicle for the PIV Credential holder. The PIV Credential provides three (3) levels of authentication:

- **Have:** individual has PIV credential/certificates on that credential that uniquely identify the holder of that credential.
- **Know:** Certificates and biometric data that are stored in the secure container of the PIV credential are protected by a strong PIN.
- **Are:** Biometrics (fingerprints, photo) are stored in the secure container of the PIV credential and protected by a strong PIN.

The Federation Assurance Level for the WidePoint PIV SSP is Not Applicable. The WidePoint PIV SSP requires in person vetting of individuals and does not have any Federation process to receive information about that individual during the vetting process. The WidePoint PIV SSP requires I-9 documentation from the individual prior to allowing PIV Credential issuance. The WidePoint PIV SSP does not federate any individual PII data post issuance. PII Data is maintained solely by the WidePoint PIV SSP as a means to prove that sufficient identifying information was gathered to allow for the creation of a PIV Credential to that individual.

### **7.3 CAN INDIVIDUALS AMEND INFORMATION ABOUT THEMSELVES? IF SO, HOW?**

Individuals may amend data about themselves as stipulated in Section 2.9.2 – PIV Card Post Issuance Update Requirements of FIPS 201-2, Section 4.8 – Certificate Modification of the FPCPF CP, and Section 4.8 – Certificate Modification of the WidePoint PIV SSP CPS. They are not able to update their data without the help of an approved Issuer that has role-based access to the system. A WidePoint PIV SSP approved Issuer must act in accordance with the provisions stipulated in the listed governing documents.

### **7.4 ARE THERE ANY PRIVACY RISKS FOR THIS SYSTEM, APPLICATION OR PROJECT THAT RELATE TO INDIVIDUAL PARTICIPATION? IF SO, HOW WILL THE WIDEPOINT PIV SSP MITIGATE THESE RISKS?**

No. Individual access is only granted through authentication of that individual's PIV credential. The WidePoint PIV SSP Issuers are the only role that can change that information post-capture.

---

## 8 SECTION 8.0 AWARENESS AND TRAINING

### 8.1 DESCRIBE WHAT PRIVACY TRAINING IS PROVIDED TO USERS, EITHER GENERALLY OR SPECIFICALLY RELEVANT TO THE SYSTEM, APPLICATION OR PROJECT.

The WidePoint PIV SSP conducts privacy and security training in accordance with the WidePoint System Security Plan, Awareness and Training Control AT-2 – Security Awareness Training which is mandatory for all employees. Employees who have access to PII contained within the WidePoint PIV SSP are in trusted roles assigned by WidePoint with executive authorization and who have undergone role-based training as outlined in the WidePoint System Security Plan, Awareness and Training Control AT-3 – Role-Based Security Training. AT-3 Role-Based Training applies to CAAs, SAs, Issuers, and Registrars. These role assignments include review of all governing policy and practice documents as previously defined.

### 8.2 ARE THERE ANY PRIVACY RISKS FOR THIS SYSTEM, APPLICATION OR PROJECT THAT RELATE TO AWARENESS AND TRAINING? IF SO, HOW WILL GSA MITIGATE THESE RISKS?

Yes. Role Based users may have access to PII Data contained within the system as stipulated earlier in Section 3.5 of this document. The WidePoint PIV SSP systems that collect PII data and issue digital certificates in accordance with the FPCPF are certified by the General Services Administration (GSA) up to FISMA-Moderate. For System Administrators and Certificate Authority Administrators that govern the operating system and the application respectively, risk is mitigated by having two-party control on all systems that contain PII data. One (1) WidePoint Certificate Authority Administrator and one (1) WidePoint System Administrator must authenticate to the system before any action can be accomplished.

---

## 9 SECTION 9.0 ACCOUNTABILITY AND AUDITING

### 9.1 HOW DOES THE SYSTEM, APPLICATION OR PROJECT ENSURE THAT THE INFORMATION IS USED IN ACCORDANCE WITH THE STATED PRACTICES IN THIS PIA?

The WidePoint SSP is audited and accredited by an independent third party in accordance with the FPKIPA Certificate Policy and the WidePoint SSP Certification Practice Statement. The audits are performed on an annual basis and submitted to the FPKIPA. WidePoint has an internal Corporate Security Auditor that reviews audit log data gathered as referenced in section 6.5 of this document, and in accordance with the certificate policy which states that logs are reviewed at a minimum every 2 months. Reports are posted to an internal share and management is notified of the report and any issues that may arise from that report.

### 9.2 ARE THERE ANY PRIVACY RISKS FOR THIS SYSTEM, APPLICATION OR PROJECT THAT RELATE TO ACCOUNTABILITY AND AUDITING? IF SO, HOW WILL GSA MITIGATE THESE RISKS?

No. Privacy data is not included in the audit and accountability reports. Audit data reports are reduced to block out user names and any personal identifying information. Audit reports are to ensure that certificates are issued properly and that the system is functioning in accordance with the System Security Plan, the Common Policy and the Certification Practice Statement.

---

## 10 APPENDIX A

WidePoint PIV SSP Memorandum of Agreement (MOA) granted by the Federal PKI Policy Authority.



### Memorandum of Agreement Federal Public Key Infrastructure

This Memorandum of Agreement ("Agreement") is entered into by the United States Federal Public Key Infrastructure Policy Authority ("Policy Authority") located at 1800 F Street, NW Washington, DC 20405 and WidePoint Cybersecurity Solutions Corporation [Personal Identity Verification Shared Service Provider] ("Entity") located at 11250 Waples Mill Road, South Tower, Suite 210, Fairfax, VA 22030 as of the date of the Policy Authority's signature to this Agreement with a term of three years. Policy Authority and Entity will collectively be referred to as "Party" or the "Parties."

#### 1. Definitions.

- a. **Public Key Infrastructure ("PKI")** is a set of policies, processes, and information technology systems used for the purpose of creating, maintaining and revoking certificates and public-private key pairs. A PKI certificate is considered trusted based on the security requirements of the systems, the adherence to the agreed upon set of issuance procedures for asserting a claimed set of identity attributes in the public certificate, and protection of the associated private key. The certificate policy or Object Identifier ("OID") asserted in the public certificate is a public assertion of adherence to the requirements defined in a Certificate Policy ("CP") and implementation practices stated in a Certification Practice Statement ("CPS").
- b. **Federal Public Key Infrastructure ("FPKI" or "Federal PKI")** is an implementation of a set of PKI policies, processes and information technology systems that provides the US Government with a common baseline to administer certificates and public-private key pairs. Federal PKI is one of several trust frameworks supporting federated trust of government devices and persons used by the US Federal Government.
- c. **Federal Public Key Infrastructure Policy Authority ("FPKIPA" or "Policy Authority")** is the Federal trust framework governance body for a set of PKI systems and associated certificates used for federated trust across and between Federal agencies and with entities that are not a US Federal Government agency for mission delivery purposes. The Policy Authority is a group of representatives from US Federal Government agencies (including cabinet-level departments) established pursuant to a charter under the Federal CIO council. It manages the policies governing the FPKI trust framework and approves or denies entities for certification into the trust framework.
- d. **Federal Public Key Infrastructure Management Authority ("FPKIMA" or "Management Authority")** is governed under the FPKIPA. The FPKIMA operates and manages the certification authorities ("CA") that comprise the FPKI root certification authorities and/or bridge certification authority for the participating Federal agencies.
- e. **Entity** is the organization operating a certification authority or non-federal trust framework certified by the Federal PKI Policy Authority. The certification is facilitated through the execution of this Agreement. The Entity is responsible for its adherence to the Agreement, as well as ensuring adherence to the Agreement by any external organization ("Entity Partner") public key infrastructure and / or certification authority system the Entity certifies.
- f. **Entity Customer** is an organization that receives end entity certificates from one of the Entity operated certification authority systems certified by the Federal PKI Policy Authority.
- g. **Entity Partner** is an organization external to the Entity that operates one or more certification authority systems that extends the Entity's trust relationship with the Federal PKI. Entity Partners inherit the requirements imposed by this Agreement through certification by the Entity.

---

## 11 APPENDIX B

WidePoint PIV SSP Authority to Operate (ATO) at FIPS 199 Moderate Impact level.

Authorization to Operate Letter



U.S. General Services Administration

MEMORANDUM FOR Cheryl Jenkins  
System Owner

FROM: Dan Pomeroy  
Authorizing Official

THRU: Pranjali Desai  
Acting Chief Information Security Officer  
General Services Administration

THRU: Joseph Hoyt  
Information System Security Manager

SUBJECT: Decision for Standard Assessment & Authorization for  
WidePoint

SYSTEM TYPE: Contractor System

DATE: October 5, 2018

A security controls assessment of the WidePoint information system has been conducted at the Federal Information Processing Standards (FIPS) 199 Moderate Impact level in accordance with National Institute of Standards and Technology (NIST) Special Publication 800-37 Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems", and General Services Administration (GSA) IT Security Procedural Guide CIO-IT Security-06-30, "Managing Enterprise Risk".

The system has been assessed by Vaultes using the assessment methods and procedures required by the system's assessment process as described in CIO-IT Security-6-30 to determine the level of risk associated with operating the system and the effectiveness of the system's security controls in satisfying the security requirements of the system. A Plan of Action and Milestones (POA&M) has been developed describing the corrective measures implemented or planned to address any deficiencies in the security controls for the information system and to reduce or eliminate known vulnerabilities.