COMPLIANCE IS MANDATORY

Responsible Office: Code V/Office of the Chief Information Officer (OCIO)

Subject: New Arrival Computer Access Process

TABLE OF CONTENTS

PREFACE

P.1 PURPOSE

This document describes the step-by-step process for providing access to a computer for new hire civil servant (CS) or support service contractor (SSC) employees. The primary intent is to provide an overview and expected timeline for a new employee to gain access to Information Technology (IT) resources at Glenn Research Center (GRC).

P.2 APPLICABILITY

a. The intended audience of this document is any GRC employee who will be employed longer than 179 days and will need access to a computer. In addition, supervisors and other process stakeholders will find information useful in expediting computer access for new hires. To promote compliance with this process, the Office of the Chief Information Officer (OCIO) requests that all individuals who need access to a computer, and any stakeholders, read, understand, and follow this overall process.

b. This Glenn Procedural Requirements (GLPR) directive is applicable to all organizations, persons working at, or visiting GRC Lewis Field and Plum Brook Station.

c. This directive is applicable to documents developed or revised after the effective date of this GLPR.

d. In this directive, all mandatory actions (i.e., requirements) are denoted by statements containing the term "shall." The terms "may" denotes a discretionary privilege or permission, "can" denotes statements of possibility or capability, "should" denotes a good practice and is recommended, but not required, "will" denotes expected outcome, and "are/is" denotes descriptive material.

e. In this directive, all documents citations are assumed to be the latest version, unless otherwise noted.

P.3 AUTHORITY

NASA Procedural Requirements (NPR) 2810.1, Security of Information Technology

P.4 APPLICABLE DOCUMENTS AND FORMS

a. Federal Information Processing Standard (FIPS) Publication 201, Personal Identity Verification (PIV) of Federal Employees and Contractors

b. NASA Form GRC 75, Space Management Committee Request

c. The Risk Designation Worksheet (https://epds.nasa.gov)

MEASUREMENT/VERIFICATION

P.5 The Office of the Chief Information Officer – IT Operations will use established FIPS 201 standards to ensure compliance.

P.6 CANCELLATION

This GLPR cancels GLPR 2810.2A, New Arrival Computer Access Process w/Change 1 (10/05/2015), dated May 27, 2015.

LAURENCE SIVIC

Digitally signed by LAURENCE SIVIC
Date: 2020.07.08 07:56:11 -04'00'

Laurence A. Sivic
Associate Director

CHAPTER 1: Badge Process

1.1 NASA Civil Servants (CS)

1.1.1 When a new CS accepts the offer to join the NASA GRC team, the NASA Shared Services Center (NSSC) in partnership with the Office of GRC Human Resources (OHR) enters the new employee's personnel information into the Workforce Transformation Tracking System (WTTS). The information from WTTS is automatically fed into the Identity Management and Account Exchange (IdMAX) system (https://idmax.nasa.gov/), which is NASA's central directory and workflow system for supporting NASA's Personal Identity Verification (PIV) workflow-oriented environment. When the new employee's record first appears in IdMAX, the new employee is identified as a PIV applicant in the context of the PIV process.

1.1.2 Risk Designation

For NASA CSs, the supervisor completes the Risk Designation Worksheet in the electronic Position Description System (ePDS). The Human Resource Business Partner (HRBP) and appropriate personnel security (PERSEC) specialist reviews and verifies the worksheet for accuracy.
The results of the Risk Designation Worksheet will identify the new employee's specific position risk and sensitivity level based on their assigned duties and will determine the appropriate level of background investigation needed.

1.2 Non-NASA Employees

For new hire non-NASA employees, the PIV identity requester manually enters information that identifies the new PIV applicant (i.e., the new hire non-NASA employee) directly into IdMAX, since the WTTS system is not applicable to non-NASA employees. The PIV affiliation workflow then notifies and sends the non-NASA employee PIV request to the PIV sponsor (typically the contracting officers' representative (COR)) for approval. After the PIV affiliation sponsor approval, the PIV workflow notifies and sends the PIV request to the PIV authorizer, who is a personnel security (PERSEC) specialist in the GRC Protective Service Office (PSO) and is responsible for initiating and adjudicating the PIV applicant's background investigation.

1.2.1 Position Designation

For non-NASA employees, the contractor human resource (HR) representative, facility security officer, or supervisor completes the IdMAX Position Designation for the employee. The Position Designation will identify the appropriate background investigation level required. This will in turn notify the PERSEC specialist in OPS who will verify the information for accuracy.

[This space left intentionally blank.]

1.2.1 Non-NASA Employee On Board Roles and Responsibilities Table

Contractor HR	PIV Identity Requestor	PIV Applicant	PIV Affiliation Sponsor	PIV Authorizer	OPS	Badge Process
	x					Manually-enters information into IdMAX
			x			Approves the request
				x		Initiates the background investigation on the PIV applicant
			x		x	Notification comes through OPS via IdMAX for approval

1.3 Investigation Requirements

1.3.1 NASA CSs

The PIV authorizer and the NSSC Suitability Agent (SA), both PERSEC specialist, researches the applicant's background investigation history. If there is a current investigation at a level equal to or higher than the position-designated investigation and the applicant has provided fingerprints at the GRC Main Gate Badging office, the authorizer will authorize, under reciprocity, the applicant and issue a permanent badge. If there is not an investigation, the investigation is not current, or it is not at the appropriate level, a new investigation shall be initiated by the NSSC SA at the NSSC. Once the PIV applicant has completed both the fingerprint requirement and the security questionnaire and the NSSC SAhas released the investigation to the Defense Counterintelligence and Security Agency (DCSA), the PIV authorizer can then authorize the applicant's permanent badge.

1.3.2 Non-NASA Employees

The PIV authorizer, a PERSEC specialist, researches the applicant's background investigation history. If there is a current investigation at a level equal to or higher than the position-designated investigation and the applicant has provided fingerprints at the GRC Main Gate Badging office, the authorizer willauthorize under reciprocity the applicant and issue a permanent badge.. If there is not an investigation, or the investigation is not current, or is not at the appropriate level, a new investigation shall be initiated by the PERSEC specialist based on the Position Designation. Once the PIV applicant has completed both the fingerprint requirement and the security questionnaire in the e-QIP system, the PERSEC specialist will review the applicant's security questionnaire for accuracy and release the investigation to the DCSA, at which time the PIV authorizer can authorize the applicant's permanent badge..

1.4 NASA Military and other Government Detailees

The appropriate human resources office or agency security office representative will notify the OPS PERSEC specialist of a current investigation for the new military or other government detailee. The PERSEC specialist will then obtain the current investigation from DCSA. The PIV identity requestor for

the specific NASA organization who is hosting the new military or other government detailee will either create a new PIV identity or modify the existing PIV identity in IdMAX. The PIV affiliation sponsor for the specific NASA organization who is hosting the new military or other government detailee will then sponsor the specific PIV request. After the hosting NASA organizational affiliation sponsor has sponsored the PIV request and the appropriate level of background investigation has been verified, the PERSEC specialist will authorize the PIV approval in IdMAX and authorize the applicant's permanent badge.

1.5 Authorization

1.5.1 Reciprocity Applicability

If the PIV applicant has a current investigation that is within scope and at a level equal to or higher than the risk designation, or is a military or other government detailee with a favorably adjudicated background investigation, the PIV applicant can be authorized due to reciprocity after submitting fingerprints at the GRC Main Gate Badging office.

1.5.2 Applicant Needing a Background Investigation

1.5.2.1 The background investigation process is comprised of two components which require the applicant to provide fingerprints at the GRC Main Gate Badging office and complete a security questionnaire in the e-QIP system. To complete the security questionnaire component, all new hire CS PIV applicants will work with the NSSC SA and all new hire support service contractor PIV applicants will work with the GRC PERSEC specialist. After completing the e-QIP security questionnaire, thePIV applicant will print, sign, and submit the e-QIP signature pages to the NSSC SA or the PERSECspecialist in OPS. In addition to completing the e-QIP process, all PIV applicants shall report to the GRC Main Gate Badging office with two valid forms of identification, one of which must contain aphotograph, to provide fingerprints and complete the PIV enrollment process on the Universal Registration Client.

1.5.2.2 In addition to an IdMAX identity, the PIV applicant will automatically be assigned a Uniform Universal Person Identification Code (UUPIC) and an Agency UserID (AUID) by the IdMAX system.

1.5.2.3 After the PIV applicant is assigned an IdMAX identity, the applicant is given ten business days to complete the security questionnaire in e-QIP and the fingerprint process. The authorization of a permanent badge is contingent on the employee's timeliness in completing the process. Once the PIV applicant completes the background investigation security questionnaire in the e-QIP system, the PERSEC specialist will review the applicant's security questionnaire for accuracy and release the investigation to the DCSA, at which time the PIV authorizer can authorize the applicant's permanent badge.

CHAPTER 2: IT Resource Account

2.1 When the new employee is in need of computing resources that require Enterprise-Managed Services delivery, there are two key items that shall be accomplished before enterprise contractor takes any action:

a. Establish a NASA Data Center (NDC) domain and NASA Operational Messaging and Directory Service (NOMAD) email accounts during the identity request process.

b. Subscribe to a new Enterprise-Managed Services device once the location has been determined.

2.2 For CS employees, the NSSC will create the employee's identity in IdMAX which establishes the associated UUPIC and AUID. Once the employee's identity record in IdMAX has transitioned to "enabled," the NDC domain and email accounts will be established. For support service contract (SSC) and all other personnel:

a. If the identity requestor does not indicate access is needed for a non-NASA Employees then the request shall be initiated manually through NASA Access Management System (NAMS). Creation of the domain and e-mail account will be provisioned immediately after the NAMS sponsor approves the request.

b. A key point to note is that the new employee shall comply with all emails from IdMAX, NSSC, and OHR.

2.3 To obtain an Enterprise-Managed Services, the IT point-of-contact (ITPOC) requires a completed NASA Form GRC 75, Space Management Committee Request, to be able to identify the location for resources to be delivered. Also, the new employee's relationship manager or ITPOC should identify the new employee's IT resource needs and order through the Enterprise Service Desk (ESD) https://esd.nasa.gov/esdportal.

2.3 IT Resource Process - Roles and Responsibilities Table

NDC	Enterprise-Managed Services	PIV Applicant	Applicant Organization	Process
			X	Identify the computing needs (computer, phones. at the earliest possible point and place a request for a service and network drop with the IT POC Click https://esd.nasa.gov/esdportal; search EUSO Ordering Guide
			X	Request a NDC domain account and NOMAD account if not requested at Identity create time
X				Establish an account for the new employee once NAMS sponsor approves request
	X			Deliver a standard seat within 5 business days and an augmented service or a workstation within 45 days after an order has been approved and received by Enterprise contractor.

CHAPTER 3: IT Security Training

3.1 The IT security training is completed in the System for Administration, Training, and Educational Resources for NASA (SATERN) at https://satern.nasa.gov/. Initial IT security training should be taken according to the onboarding process and renewed annually.

3.1.1 For NASA CSs, obtaining a SATERN account happens when the WTTS record is published.

3.1.2 Before SSC employees can login to SATERN, they shall first create their profile in Launchpad (https://auth.launchpad.nasa.gov/). The employee should receive information on this process from their employer and can perform this on their first day. Learning Center computers and staff are available to assist with account set-up. Once their account is active (generally 24 hours later) the SSC employee is able to login to SATERN and complete the required training modules.

a. The SSC(s) may create their own accounts directly in SATERN. A new contractor employee is able to set up their account by following the instructions on the SATERN home page.

b. The SSC is responsible for ensuring each of their employees take the IT security training.

3.2 The table below identifies the critical tasks of this phase and the parties responsible for each task.

3.2 IT Security Training Roles and Responsibilities Table

NSSC	Contractor	Learning Center	IT Security Training
X			Publish employee in WTTS so SATERN account is created
	X		Create their own accounts through SATERN
	X		Responsible for the contractor to take the IT security training
		X	Assist new contractors set up their account per the instructions on the SATERN home page

Appendix A: Definitions

Personal Identity Verification (PIV) Applicant. Individual who need access to NASA resources, such as information technology systems or facilities.

PIV Authorizer. Authorizes the issuance of a PIV card to a PIV applicant who has met all proofing, enrollment, and investigative requirements.

PIV Enrollment Official. Validates the PIV applicant's identity and captures identity information and biometrics.

PIV Issuance Official. Encodes, finalizes, and issues the badge to the PIV applicant.

PIV Identity Requestor. Provides initial data about a PIV applicant and submits the PIV request on behalf of the PIV applicant.

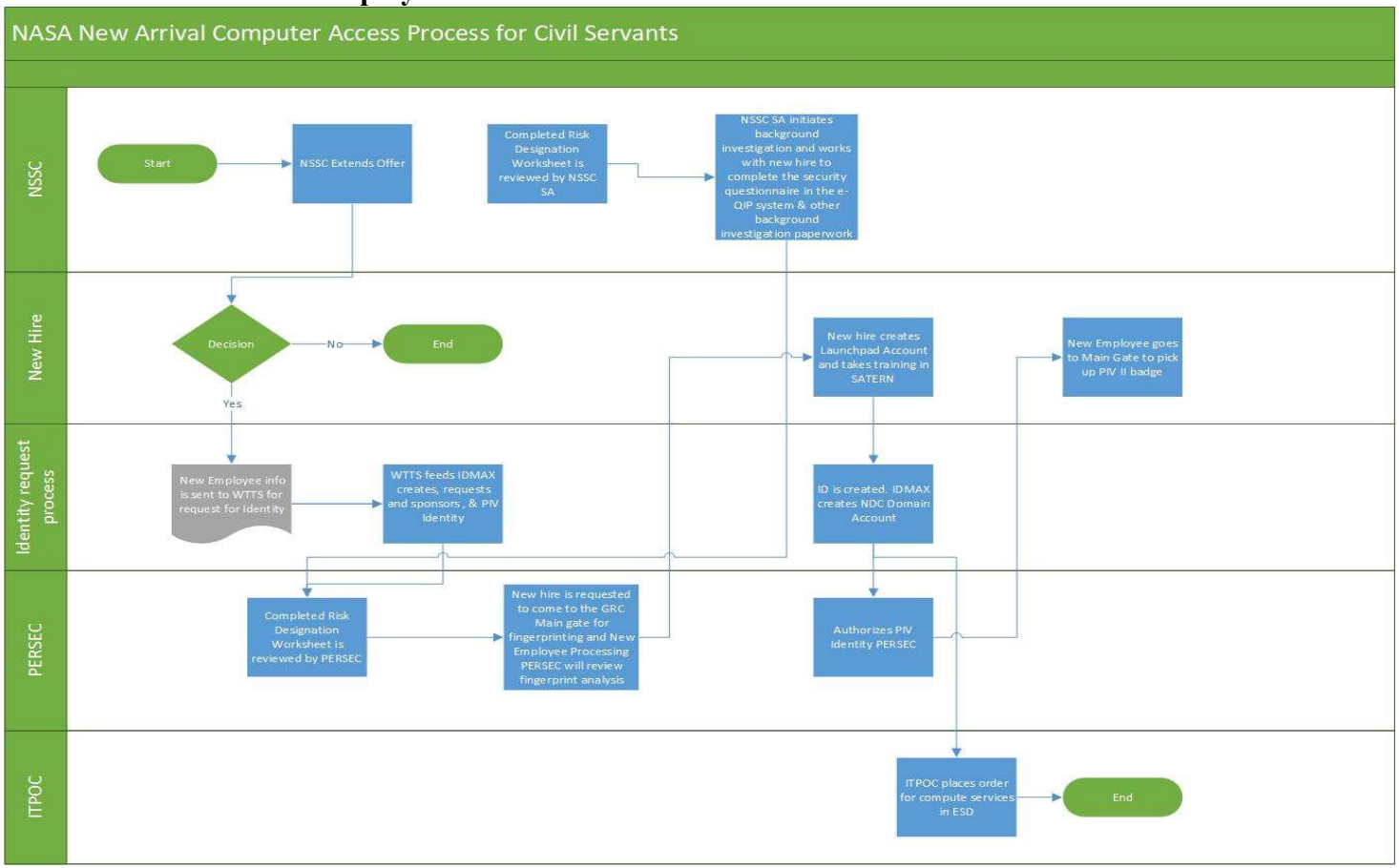
PIV Affiliation Sponsor. Validates the relationship between the PIV applicant and NASA.

Appendix B: Acronyms

AUID	Agency UserID
COR	Contracting Officer's Representative
CS	Civil Servant
DCSA	Defense Counterintelligence and Security Agency
EOD	Enter on Duty
ESD	Enterprise Service Desk
ePDS	electronic Position Description System
eQIP	Electronic Questionnaire for Investigation Processing
EUSO	End User Services Office
FBI	Federal Bureau of Investigation
FIPS	Federal Information Processing Standard
GLPR	Glenn Procedural Requirements
GRC	Glenn Research Center
HR	Human Resources
HRBP	Human Resource Business Partner
IdMAX	Identity Management and Account Exchange
IT	Information Technology
ITPOC	Information Technology Point of Contact
NAMS	NASA Access Management System
NDC	NASA Data Center
NOMAD	NASA Operational Messaging and Directory Service
NPR	NASA Procedural Requirements
NSSC	NASA Shared Services Center
OCIO	Office of the Chief Information Officer
OHR	Office of GRC Human Resources
OPS	Office of Protective Services
PERSEC	Personnel Security
PIV	Personal Identity Verification
SA	Suitability Agent
SATERN	System for Administration, Training, and Educational Resources for NASA
SSC	Support Service Contractor
UUPIC	Uniform Universal Person Identification Code
WTTS	Workforce Transformation Tracking System

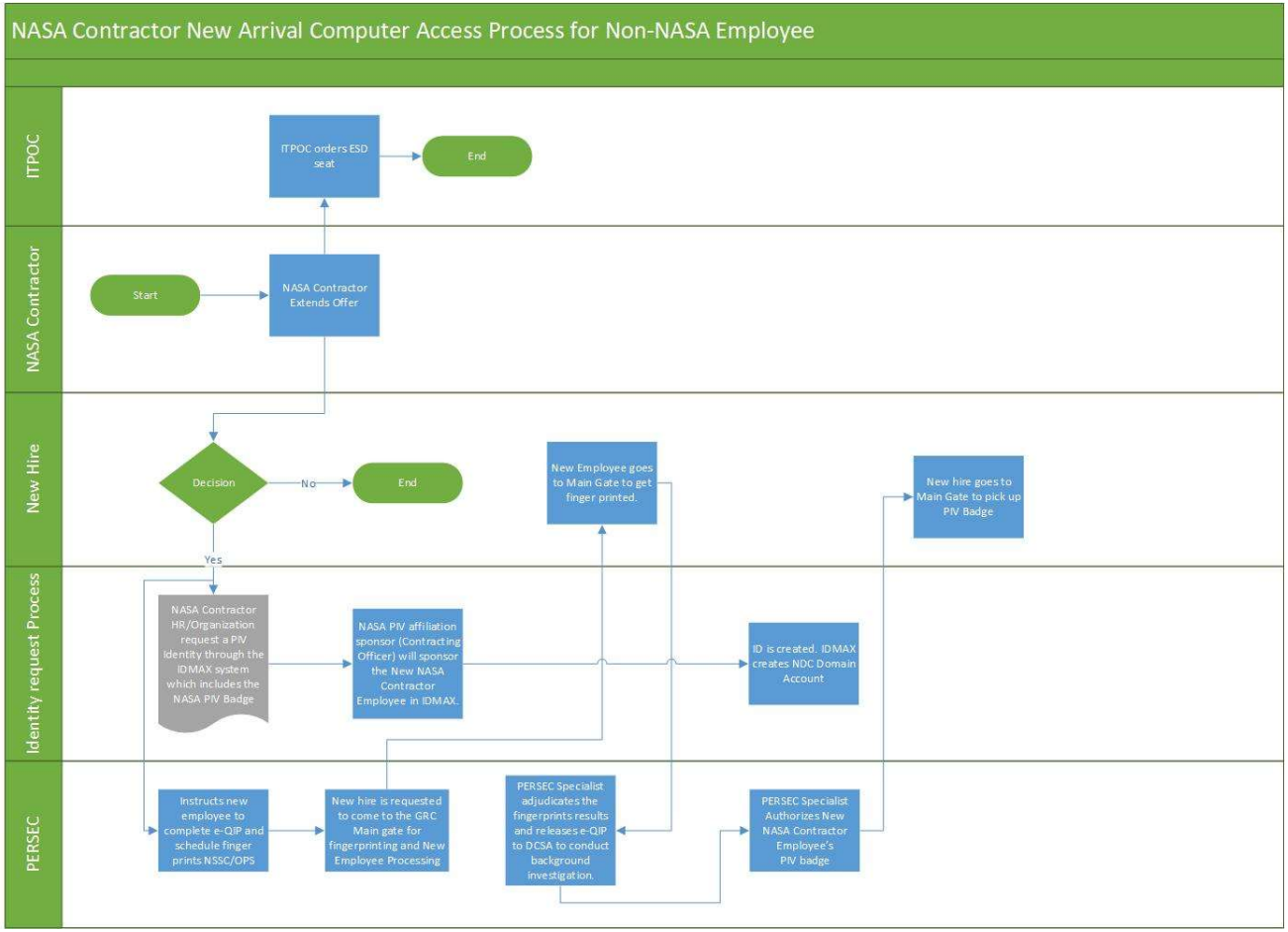
Appendix C: New Arrival Computer Access Process

C.1 NASA Civil Service Employee



Appendix C: New Arrival Computer Access Process (continued)

C.2 Non-NASA Employee



Appendix D: Timeframe

D.1 NASA Civil Service Employee

Sponsor	Responsible Duty	Timeframe
New hire employee	• Accepts offer • Goes to Main Gate Badging Office for fingerprinting • Goes to Main Gate Badging Office to pick up badge	• Received no later than 4 weeks prior to EOD on EOD • Within 1 business day after the PIV identity has been authorized
New Hire Org	• Orders Enterprise-Managed Services seat	• Delivery within 5 business days after the orders went through the approval cycle in Servicenow
NSSC/PERSEC Specialist	• Instructs new hire to complete e-QIP and schedule fingerprints (NSSC) • Authorizes PIV identity (OPS)	• No later than 10 business days prior to their EOD date • Within 3 business days after investigation results received
IdMAX	• Auto-Provisions account	• When WTTS data is published
System Administrator	• Enables an account	• Within 3 -5 days after account request
FBI, DCSA	• Process fingerprints and initiates background investigation	• Within 5-12 business days after submittal of package

Appendix D: Timeframe (continued)

D.2 Non NASA Employee

Sponsor	Responsible Duty	Timeframe
New hire employee	• Accepts offer • Goes to Main Gate Badging Office for fingerprinting • Goes to Main Gate Badging Office to pick up temporary badge	• Received no later than 12 days prior to EOD • Any time after PIV identify is sponsored but no later than EOD • Within 1 business day after the PIV identity has been enabled
New Hire Org	• Orders Enterprise managed service (devices)	• Delivery within 5 business days from ordering services seats
Contractor HR	• Enters information into IdMAX	• No later than 10 business days prior to EOD • No later than 10 business days prior to EOD
COR	• Sponsors PIV identity	• Within 10 business days of new hire's identity being created • No later than 10 business days prior to EOD
PERSEC Specialist	• Instructs new hire to complete e-QIP and schedule fingerprints • Enables PIV identity	• No later than 10 business days prior to their EOD date • Within 3 business days after fingerprints results received
Account Administrator	• Requests an account	• Within 5 business days after PIV identity enabled
System Administrator	• Enables an account	• Within 3 -5 days after account request
FBI, DCSA	• Process fingerprints and initiates background investigation	• Within 5-12 business days after submittal of package

Change History

Change	Date	Description/Comments
Basic	4/8/09	New Directive Baseline
Change 1	5/4/09	Corrected errors within flowchart A in Appendix B
Change 2	4/13/10	Updated Chapter 3 (schedule for taking training; from 30 days to 90 days) per previously released guidelines
Change 3	4/15/14	Added a 12-month extension to the expiration date (from 4/8/14 to 4/8/15) in accordance with GLID 1410.7
Change 4	4/6/15	Added a 12-month extension to the expiration date (from 4/8/15 to 4/8/16) in accordance with GLPR 1410.1 (revised directive was entered into official review.)
A	5/27/15	Updated Chapter 3 to reflect current practice and updated flowchart. Added an appendix for acronyms. Updated format/content per NPR 1400.1
Change 1	10/5/15	Changed responsible organization from Code VM/Information Technology Mission Support Office to Code V/Office of the Chief Information Officer (CIO)
B	7/08/2020	• Updated to meet requirements of GLPR 1410.1; new template • Chapter 1: Badge Process. 1.1.1 – Changed the Office of the Chief Human Capital Office (OHR) Management (OHCM) to NASA Shared Services Center (NSSC) in partnership with the Office of GRC Human Resources (OHR) • 1.1.2 – changed OHCM classification officer to The Human Resource Business Partner (HRBP). Change the table to reflect the information. • 1.2 – add "identify" after PIV. Changed Civil Servants to NASA Employees • Add "affiliation" before sponsor. • 1.2.1 – change the word Risk to "Position". Revised the section to reflect current practice. • 1.3 Reflects current practice and updated the table. • Chapter 2 IT Resource Account - Reflects current practice and updated the table. • Chapter 3 IT Security Training - Reflects current practice and updated the table. • Appendices: Updated the tables and acronyms to reflect current practice • Appendix C: renamed to "New Arrival Computer Access Process Flowcharts"