PRIVACY IMPACT ASSESSMENT— FEBRUARY 2023

# Identity, Credential and Access Management (ICAM)

| | |
|---|---|
| **Does the CFPB use the information to benefit or make a determination about an individual?** | No. |
| **What is the purpose?** | A program and suite of tools to manage access and authentication to CFPB IT resources. |
| **Are there controls to enforce accountability?** | Yes, all standard CFPB privacy protections and security controls apply. |
| **What opportunities do I have for participation?** | Generally applicable: Appropriate opportunities for notice, consent, access, and redress. |

Consumer Financial Protection Bureau

# Overview

The Dodd-Frank Wall Street Reform and Consumer Protection Act (the Act), Public Law No. 111-203, Title X, established the Consumer Financial Protection Bureau (CFPB). The CFPB relies upon diverse information technology (IT) systems and applications used by CFPB staff and external parties to perform their duties. CFPB implements a comprehensive Identity, Credential, and Access Management (ICAM) program to centrally manage access to these applications and systems, and to safeguard the data CFPB collects, uses, shares, and maintains. The ICAM program collects information to verify individuals' identities, establish a digital identification (ID), and grant privileged access to CFPB data to complete their responsibilities.

The ICAM program centrally manages all staff (i.e., employees, contractors, detailees, volunteers, and interns) identification, authentication, and access privileges to all CFPB systems. It also manages the provisioning of access to CFPB IT resources by authorized external individuals. The ICAM program manages a suite of enterprise tools and applications to create and manage digital IDs and access to CFPB IT resources. CFPB uses these tools to help reduce costs, manage IT security risk, enable new business opportunities, and improve compliance. These tools and applications also support CFPB's alignment with functional areas mapped to the Cybersecurity & Infrastructure Security Agency (CISA) Identity Capability functions. The CFPB ICAM program comprises three structural areas:

- Identity Governance and Administration – Monitors and ensures that user identities and access rights remain properly managed, secure, and monitored. It also provides insight into who has access to systems and PII based upon a defined role and responsibility.
- Authentication & Authorization – Verifies staff identity and limits what actions CFPB staff can perform after access is granted.
- Privileged Access Management – Focuses on the protection of privileged accounts at the CFPB where elevated access to systems and PII is managed using CFPB Rules of Behavior (RoBs) and Privilege User Access Requests (PUA) within specific environments. RoBs and PUAs are approved by system owners.

Authorized CFPB program managers, business owners, system developers, system owners, and other internal CFPB users can access these tools and applications to support and manage the agency's identity management need, such as deployment of two-factor authentication methods, and provisioning restricted and temporary access to CFPB data and resources.

The ICAM program requires the collection and use of personally identifiable information (PII) to operate, which is stored in a centralized identity management data hub. The PII is collected from internal data sources, such as the CFPB Automated Background Investigation System (ABIS)[1] and external resources hosted by federal agencies such as HR Connect, USAccess, Active Directory, Login.gov, and from external individuals. The ICAM program uses PII from these various sources to provision accounts, coordinate and execute access requests and approvals, automate onboarding, transfer access between systems, and review access permissions across the enterprise. The CFPB uses the PII to verify an individual's identity and confirm they are cleared through the appropriate security or background (conducted by the appropriate federal agencies on behalf of CFPB), and thus authorized to access our IT systems and network. The PII is also used to assign a single digital trusted identity, such as a username, to authenticate individuals when logging into CFPB system[2]. Additionally, the PII allows the ICAM program to verify individuals each time an attempt is made to log into an IT system and monitor and manage these digital identities at the request of an individual, or as approved by a system owner.

The CFPB is conducting this privacy impact assessment (PIA) to assess the ICAM program's use of PII stored within the centralized data hub and used within the tools and applications to identify the associated privacy risks. The scope of this PIA is limited to the privacy risks and technical controls related to the maintenance and use of PII to support ICAM program activities. Specific tools and applications, such as automated PUA forms, are used to analyze the collection and use of PII with each system and user requesting access and these processes are documented within system-specific PIAs such as the CFPB Automatic Background Investigation System. The CFPB's authority to collect specific information and routine uses of those records are identified in the

[1] The Automated Background Investigation System (ABIS) https://files.consumerfinance.gov/f/documents/cfpb_automated-background-investigation-system-abis-pia_2021-03.pdf

[2] Or in the case of Login.gov, it creates a single digital trusted identity across multiple federal systems and services.

associated Systems of Records Notices (SORN)[3]. Program-specific uses of data that require Paperwork Reduction Act (PRA) approval will also be documented within the corresponding system-specific PIAs. Records are maintained in accordance with the applicable records retention schedule and are generally subject to National Archive and Records Administration (NARA) General Records Schedules (GRS) GRS 1.1, GRS 1.2, GRS 2.1, GRS 2.2, GRS 2.3, GRS 2.4, GRS 2.5, GRS 2.7, GRS 5.6, GRS 5.7, and GRS 6.4 depending on the record type and the corresponding disposition of that record type, and as specified within applicable SORNs.

The PII used by the ICAM program is collected in accordance with the Dodd-Frank Act, Homeland Security Presidential Directive (HSPD) 12, NIST Federal Information Processing Standard (FIPS) 201-3, Person Identity Verification (PIV) of Federal Employees and Contractors, January 2022, Office of Management and Budget (OMB) M-19-17, and the Privacy Act of 1974. Changes within the ICAM program, which includes all the tools and applications utilized within the program, are managed through CFPB Change Control Board (CCB) processes and A&A documentation and address privacy to include functional requirements analysis, alternatives analysis, feasibility analysis, benefits/cost analysis, and privacy risk assessments.

# Privacy Risk Analysis

The primary privacy risks associated with PII are related to:

- **Data Quality and Integrity**
- **Data Minimization**
- **Limits on Uses and Sharing of Information**
- **Security**
- **Accountability and Auditing.**

**Data Quality and Integrity**

The ICAM program itself collects a very little amount of PII directly from individuals. The majority of PII collected by the program comes from other systems, applications, and associated processes such as human resources, onboarding data, and other federal government ICAM programs such as Login.gov and USAccess. This presents a risk that PII

[3] One of these SORNS includes the GSA/GOVT-7, HSPD-12 USAccess, which covers all participating agency employees, contractors and their employees, consultants, and volunteers who require routine, long-term access to federal facilities, information technology systems, and networks. *See also* OPM/GOVT-1, General Personnel Records; OPM Central-9, Personnel Investigations Records.

may be inaccurate when sourced by the ICAM program. The ICAM program mitigates this through implementation of procedures such as two-factor authentication, where individuals must validate their identity by providing a 'thing they know' (such as a password or personal identification number), a 'possession' (such as an ID badge or token on a smartphone), 'something you are' (username or email), and/or location. In addition, the ICAM program reviews all access requests approved by system owners via PUAs to determine the type of access required. If information in the PUA does not match the information sourced by the ICAM program for verification, the individual is not granted access.

### Data Minimization

PII collected by the ICAM program enables the CFPB to provision access to its systems and applications. PII is collected from internal data sources, such as the CFPB ABIS, external resources hosted by federal agencies such as HR Connect, USAccess, Active Directory, Login.gov, and from external individuals. Each of these sources contain a varying amount of PII. As a result, there is the risk that the program may collect more PII than is necessary to grant access. To mitigate this risk, the ICAM program utilizes digital forms that collect only the minimum amount of PII necessary from source systems to build a digital identity, verify an individual's identity, and grant access to CFPB systems. Once these forms are completed, the ICAM program builds an individual's digital identity within a centralized data hub. When an individual receives a digital identity, access can then be assigned by the ICAM program. System and data access just first be approved by a CFPB system owner before access is provisioned by the ICAM program.

If more than the necessary amount of PII is provided to the ICAM program, ICAM program staff removes unnecessary PII before using the data to conduct program activities. Further, the ICAM program centrally manages the identities of individuals to prevent the need to continually collect PII to identify individuals for requested access to individual systems.

### Limits on Uses and Sharing of Information

The ICAM program collects PII about all CFPB staff and authorized external individuals to provision access to CFPB IT resources. The amount of information collected presents a risk that PII can be used for unauthorized purposes. The ICAM program mitigates this risk through automated access requests processes, such as PUAs, that limit the amount of PII used to verify an identity and provision access to the system. As part of this process, the system owner is an approver, ensuring that the individual is approved for access before the ICAM program grants access to the system or application. The ICAM program also does not share any PII with any unauthorized individual in accordance with cybersecurity and privacy policies.

### Security

Given the sensitivity of PII collected and used by the ICAM program, the program's tools and applications may be a target for unauthorized access. To mitigate this risk, the ICAM program tools and applications are subject to the appropriate technical, physical, and administrative controls issued by the National Institute of Standards and Technology (NIST) to identify, analyze, prioritize, and remediate risks. Security and privacy controls are implemented to restrict access to PII to authorized individuals who support the ICAM program. CFPB also has implemented security tools that can be configured to scan ICAM systems to detect malware, phishing, spam, and unsafe links. The ICAM program also uses audit logs to audit login attempts and other such events as specified by the CFPB's Cybersecurity Enterprise Standards Manual (CS-S-01)[4]. Finally, access to the ICAM program tools and applications is strictly reviewed, approved, and maintained by the ICAM program leadership.

### Accountability and Auditing

The ICAM program must ensure that authorized CFPB personnel have the right access to the right CFPB resources based on their roles. There is a risk that the ICAM program may inadvertently mishandle the PII it collects from CFPB staff by sharing it with an unauthorized person due to a gap in knowledge of CFPB procedure. To ensure these risks are mitigated, the ICAM program must complete annual role-based training on identifying various CFPB roles and the accompanying access to be granted, handling CFPB PII, and information security. The training covers topics to ensure the ICAM program is equipped to run checks that certify a person has the right access in the right role and that this access does not inadvertently grant the individual access to other roles or to other systems.

For all other CFPB users who have been granted access to CFPB systems, the CFPB 's RoB provides guidance and specific rules on the appropriate use of CFPB information systems for individuals. Users must review, acknowledge, and sign that they understand the CFPB's RoB. Users are also only authorized to receive the minimal level of access required to accomplish assigned core job functions. For example, individuals requiring administrator rights to a system where said rights would be considered above that of a normal user must complete the PUA request and undergo reviews and approvals before access is granted. Finally, internal new-hire and annual training and guidance for managing PII apply to all who work for the CFPB, including vendor staff. The training includes recognizing possible breaches of PII and how to report them. The ICAM program works with system owners and employs both

[4] CFPB Cybersecurity Enterprise Standards Manual (CS-S-01) (Appendix F: CFPB Auditable Events)

automated and manual processes to review and validate continued access to CFPB systems and applications. Additionally, both internal and independent auditors hold the CFPB accountable for complying with CFPB policies and procedures related to the processing of PII. The CFPB is committed to taking swift and immediate action if we uncover any violations of law, policies, and procedures.

The technical, physical, and administrative controls implemented to promote individual participation, minimization, and accountability are appropriate and implemented within the ICAM program and within program-specific PIAs.

# Privacy Risk Management

## 1. Describe what information the CFPB collects, how the information is collected, and the sources from which the information is collected.

The ICAM program collects a very limited amount of PII directly from individuals by allowing customization of their CFPB digital identity profile, such as their preferred job title, preferred pronouns, and a primary phone number such as a personal cell number and personal address if the individual works from home. The ICAM program primarily uses PII collected by indirect sources such as CFPB employment applications and contractor onboarding forms housed within ABIS[5] and HR Connect[6], and from other federal agency sources such as USAstaffing[7], USAccess[8], and Login.gov. Information from these sources is collected via an application programming interface (API), and through other secure data transmission methods, and flat text files to connect the centralized ICAM data hub to these data sources. The PII collected by the ICAM program is primarily used to verify an individual identity to create a digital ID. Once a digital ID is created,

[5] CFPB's internal system which supports the prescreening and adjudicating of background investigations and security clearances. ABIS Privacy Impact Assessment (PIA) can be found at https://files.consumerfinance.gov/f/documents/cfpb_automated-background-investigation-system-abis-pia_2021-03.pdf

[6] Treasury-owned and operated human resources systems utilized by the CFPB to manage human resource processes efficiently and easily.

[7] Office of Personnel Management's staffing system leveraged by the CFPB to meet its recruitment activities.

[8] Federal government shared PIV service leveraged by the CFPB to support issuance of PIVs and other credentialing services.

PII is subsequently used by the ICAM program for purposes such as authorization decisions for system access, manage group/role memberships, and create dashboards such as PIV login enforcement metrics. The PII collected may include:

- Full name;
- Social Security Number;
- Date of birth;
- Place of birth;
- Citizenship status;
- Position number and description;
- Employee number or ID;
- Supervisory status;
- Work location;
- Address (business or personal);
- Email address (business and personal);
- Phone number (business and personal);
- Selective service registration;
- Demographic information;
- Military service history;
- Residential address;
- Background investigation adjudication details;
- Present and previous employer information;
- Manager or Contracting Official Representative (COR)/Assistant COR (ACOR);
- Contract numbers and validity dates;
- Date of employment start;
- Entry on duty date;
- Declaration of relatives employed by the CFPB;
- Work division, department (Office), and section;
- Personnel type (employee, contractor, volunteer, detailee, auditor, intern)
- Bargaining unit eligibility status, as applicable;
- Job code, title, pay grade, pay plan, occupational series;
- PIV Sponsorship status, date;
- PIV card user principal name;

- PIV card and certificate status;
- PIV enrollment status, date;
- PIV card serial number and cardholder unique identifier (CHUID);
- Credit card expiry date and Serial Number;
- School transcripts;
- Training compliance data.

The ICAM program manages tools and applications that allow the CFPB granular control of systems and access to PII, such as restricting access to those with a need to know based upon a role or responsibility and deployment of multi-factor authentication processes to CFPB systems. The type of PII that CFPB collects, the sources of those collections, the uses of PII, and how PII is minimized to the amount necessary are defined by system owners. Individuals complete a PUA which is reviewed and approved by the system owner, then submitted to the ICAM program for provisioning access. The type of and uses of PII are further defined in system and application-specific PIAs that can be found on the CFPB's website[9]. These systems may refer to the use of ICAM program tools and applications to provision and manage access and use of PII within CFPB systems.

As a result of this assessment, the CFPB Privacy team is now part of governance and project working groups to assess privacy implications using ICAM program tools and applications.

## 2. Describe CFPB's objective for the information.

The ICAM program uses PII to verify identities and to assign appropriate access to CFPB systems and applications. Specifically, the ICAM program uses PII to achieve the following objectives:

- Issuing, validating, maintaining, and terminating user identities and credentials based on assigned roles and responsibilities.
- Controlling how users are granted or denied access to CFPB resources through authentication, authorization, and auditing individual accounts.
- Identifying, tracking, and managing authorized users' access to CFPB systems.
- Issuing physical hardware, such as tokens or digital keys, that are used to generate personal identification numbers (PIN) codes that help confirm an individual's identity.

[9] Please see https://www.consumerfinance.gov/privacy/privacy-impact-assessments/.

- Assigning specific access permissions to CFPB IT resources based on specialized roles and responsibilities.
- Transferring the identity and authentication of a user across CFPB's systems after a trust relationship has been established between those systems (federated SSO).

The ICAM program collects the minimum PII to identify an individual and provide the right level of access to systems. Each data element is selected based upon a need to know for the purpose of confirming an individual's identity and role within CFPB. This helps establish and maintain a unique record for each user. PII is not used for any other purpose.

## 3. Describe how CFPB shares any of the information with third parties with whom the CFPB shares the information for compatible purposes, e.g., federal or state agencies, the public, etc.

The ICAM program serves as an authoritative source of identity information to other systems owned and operated by the CFPB. The ICAM program is supported by a suite of tools and applications that provide a range of ICAM services. CFPB also shares PII with other federal agency hosted systems such USAccess, to validate an individual's identity prior to building a digital ID. For example, the ICAM program shares individuals' work email address and business telephone number with HRConnect to verify and manage PIV functions. When the ICAM program provides access to other federal agencies a work email address is shared to validate an individuals' access into a CFPB system. Any PII shared with other federal agencies and authorized third-parties is covered by memoranda of understanding (MOUs) and information sharing agreements (ISA), and are individually assessed in accordance with federal law and guidance. In instances where the CFPB shares PII maintained within the ICAM program with third parties, that information is only shared with consent from the impacted individuals or when CFPB otherwise has the authority to do so, pursuant to routine uses published in CFPB SORNs. Sharing of this information by the CFPB is covered by and consistent with the routine uses published in OPM SORN GOVT-1, General Personnel Records, CFPB.014, Direct Registration and User Management System SORN, and CFPB.009, Employee Administrative Records.

## 4. Describe what opportunities, if any, individuals to whom the information pertains must (a) receive notice regarding the CFPB's use of the information; (b) consent to such use; (c) access the information that pertains to them; or (d) obtain redress.

The ICAM program collects a very limited amount of PII from individuals for the purpose of customizing a digital identity profile. Individuals have full access to their digital identity profile to add, edit, or delete PII such as preferred job title, preferred pronouns, and a primary phone

number such as a personal cell number and personal address if the individual works from home. Information is collected from other sources, such as employment applications and contractor onboarding forms and applications, or through PUAs. The ICAM program provides notice on the collection and use of PII through the publication of this PIA, OPM SORN GOVT-1, General Personnel Records, associated SORNs[10], and Privacy Act Statements and notices, as applicable. When practicable and/or required by law, the CFPB provides notice of the uses of PII and the opportunity to consent to uses at the time of collection. Because the ICAM program uses information provided from different authoritative data sources, notice is provided at the source of collection[11]. For example, when candidates for federal employment complete a form like Optional Form (306), Declaration for Federal Employment, notice is provided at the point of collection on that form. Generally, notice is provided on the CFPB's various physical and electronic forms during employee recruitment and onboarding.

Where applicable, CFPB allows individuals to request access and amendment to their PII in accordance with the Privacy Act and CFPB's Privacy Act regulations, at 12 C.F.R. 1070.50 *et seq.* Information about Privacy Act requests is published in the associated SORNs and on the Bureau's website.[12] Employees and contractors may also be able to directly update their information.

For additional information and analysis related to specific systems, applications, and data collections, applicable SORNs, and program-specific privacy impact assessments are available at www.consumerfinance.gov/privacy.

## 5. Explain the standards and relevant controls that govern the CFPB's—or any third party contractor(s) acting on behalf of the CFPB—collection, use, disclosure, retention, or disposal of information.

The CFPB manages risks to privacy by complying with the Privacy Act of 1974, Right to Financial Privacy Act, and the E-Government Act of 2002. To further compliance, it voluntarily adopts

[10] CFPB.014, Direct Registration and User Management System SORN and CFPB.009, Employee Administrative Records found at https://www.consumerfinance.gov/privacy/system-records-notices/.

[11] An example is the Automated Background Investigation System which provides notice at collection and by its published PIA. Found at https://files.consumerfinance.gov/f/documents/cfpb_automated-background-investigation-system-abis-pia_2021-03.pdf.

[12] *See* Submit a FOIA or Privacy Act Request, https://www.consumerfinance.gov/foia-requests/submit-request/; Amending and Correcting Records Under the Privacy Act, https://www.consumerfinance.gov/privacy/amending-and-correcting-records-under-privacy-act/.

Office of Management and Budget privacy-related guidance as best practice[13] and applies the National Institute of Standards and Technology risk management processes for privacy.

The CFPB uses the following technical and administrative controls to secure PII and provide accountability for the appropriate collection, use, disclosure, and retention of personal information:

- Audit logs and reviews are in place to identify, review, and assess unauthorized access to ICAM systems and the PII that resides within its systems.
- The CFPB's general privacy training and role-based privacy training are required before granting access to the ICAM environment and any systems within the environment. Role-based training includes topics such as PII handling procedures, incident and breach response procedures, and the CFPB's authority to collect and use information in accordance with its regulations. Training completion is tracked and may be used as a determining factor to grant access to systems and applications. Further, if training requirements, such as annual training, are not met by the established deadline, the ICAM program may terminate access to CFPB systems and applications.
- CFPB incident response procedures and breach response procedures are in place to address incidents involving PII residing in the ICAM program.
- Compliance with CFPB cybersecurity and privacy policy and standard operating procedures are documented within the security and privacy implementation plans.
- Data quality and integrity checks are performed in accordance with the Bureau's Data Access Policy. The ICAM program uses PII to verify an individual's identity prior to granting any type of access to CFPB IT systems.
- The CFPB is responsible for assigning and maintaining roles and permissions within the ICAM program and its systems based on an individual's role within the organization and as approved by Cybersecurity. Any access granted to authorized individuals is reviewed periodically to determine if access is still required and, if not, disabled and removed. This includes:

[13] Although pursuant to Section 1017(a)(4)(E) of the Consumer Financial Protection Act, Pub. L. No. 111-203, the CFPB is not required to comply with Office of Management and Budget (OMB)-issued privacy guidance, it voluntarily follows OMB privacy-related guidance as a best practice and to facilitate cooperation and collaboration with other agencies.

- Administrator access is reviewed and approved by the ICAM program for all ICAM tools that are authorized and support program processes.
- Roles and responsibilities for access to CFPB systems are documented within PUAs and require system owner approval before the ICAM program grants access to CFPB systems and data.
- ICAM program staff must complete PUAs that are approved by ICAM program leadership before access is granted to ICAM tools and applications.

- Records Schedules submitted to and approved by National Archives and Records Administration (NARA) are in place for each collection of data at the system level. Systems that collect, use, maintain, and/or share PII may retain records indefinitely until the NARA approves the CFPB's records disposition schedule. Records that fall under a general records schedule are maintained and disposed of according to the applicable schedule identified within program-specific PIAs and SORNs as cited within this PIA.
- Personnel Security, including background checks, is completed for all employees, contractors, or individuals authorized to complete CFPB activities within the ICAM program.

Program-specific technical and administrative controls to secure PII and create accountability for the CFPB's appropriate collection, use, and disclosure are further documented in program-specific PIAs. The CFPB may use contractors to help support the collection, use, disclosure, or retention of information covered by this PIA, and those contractors are subject to similar controls. For example, contractors with access to direct identifying PII must report suspected or confirmed privacy incidents to the CFPB immediately and no later than one hour after discovery. Other requirements placed on contractors may include training on privacy and compliance with federal privacy requirements and Federal Acquisition Regulations (FAR). The CFPB also has procedures in place to terminate or restrict access for individuals who no longer have a need to access information in the CFPB's ICAM program because of a termination or resignation.

As a result of conducting this PIA the Privacy team removed references to the ICAM systems and applications that support the ICAM program from the existing Infrastructure General Support System PIA. This PIA now identifies the uses of PII and associated risk applicable to the ICAM program.

## 6. Discuss the role of third party(ies) that collaborate or partner with the CFPB, if any. Identify any controls used to protect against inappropriate collection, use, disclosure, or retention of information. (This does not include third parties acting on behalf

of the CFPB, e.g., government contractors discussed in Question 5.)

The ICAM program employs third-party tools and applications provided by vendors that support CFPB's ICAM program. CFPB employees and contractors supporting the ICAM program are provided access to these ICAM tools and applications. Authorized vendor staff may also have access to these tools and applications to provide development and maintenance. No other systems or individuals have access to the PII in the ICAM program. Uses of systems is managed through a project governance lifecycle where the scope and design of the system are assessed by the CFPB's security and privacy teams to ensure compliance with CFPB policies and procedures. In addition, where the ICAM tools and applications connect with other third-party cloud services, those services are also reviewed to ensure compliance. Typically, third-party tools and services providers must also be assessed in accordance with a Security Implementation Plan (SIP) identifying the necessary controls and achieving a separate Authority to Operate (ATO) prior to providing services within the ICAM program. Depending on the connection, typical controls include:

- Memoranda of understanding, information sharing agreements, and authority to use describe the collection, use, maintenance, and sharing of any PII contained within ICAM and any third-party vendor.
- Documented vendor compliance with CFPB cybersecurity policy and procedures.
- Audit logs and reviews policy and standard operating procedures.
- Role-based access controls.

In support of vendor integration and troubleshooting, the ICAM program may screen share or send log files to a support vendor analysis. Sharing of this nature is covered within non-disclosure agreements and security and privacy terms of service agreements in place as part of the contracted service, and vendors do not have direct access to CFPB systems.

# Document control

## Approval

CHRISTOPHER CHILBERT

Digitally signed by CHRISTOPHER CHILBERT
Date: 2023.03.08 17:45:21 -05'00'

Chris Chilbert

Chief Information Officer

Date

Kathryn Fong

Digitally signed by Kathryn Fong
Date: 2023.03.08 17:53:31 -05'00'

Kathryn Fong

Acting Chief Privacy Officer

Date

JOSEPH GILCHRIST

Digitally signed by JOSEPH GILCHRIST
Date: 2023.03.02 08:30:46 -05'00'

Name

Joe Gilchrist

Initiative Owner

Date

# Change control

| Version | Summary of material changes | Pages affected | Date of change |
|---|---|---|---|
| | | | |
| | | | |