cfpb

CONSUMER FINANCIAL PROTECTION BUREAU

ELEVATED/PRIVILEGED USER ACCESS REQUEST

*This is a keyboard-friendly form. Press **Tab** to move forward and **Shift+Tab** to move back. You can use the **space bar** to select buttons and **arrows** to mark check-boxes. Enter dates, phone numbers, etc., using **numbers only** (slashes and dashes added automatically). When **digital signatures** are applied, corresponding date fields are removed.*

1. Requester Information

1. FULL LEGAL NAME: **Wei Chen**

2. PHONE: (202) 760-1147

3. WORK LOCATION: Remote

4. TEAM/OFFICE: T&I

5. APPLICATION/SYSTEM NAME (separate each one with a semicolon):

JETS

6. BUSINESS JUSTIFICATION:

To maintain situational awareness as cybersecurity team member

Please provide a detailed justification for each Application/System being requested.

ACCESS TYPES

***PRIVILEGED access** is defined as requiring administrator rights to a system or application where said rights would be considered above that of a normal system user. This would include administrative access to servers or systems that would allow you to alter the operating system or applications installed in some way. Sudo rights, domain administrator and local server administrator fall into this category.*

***ELEVATED access** includes service accounts for automation purposes that do not require administrative privileges to a system or application, but need to be able to read a file or copy data to or from a file system and can also include modifying abilities on general user accounts where administrative access is not required.*

2. General Systems — Privileged Access

— Check all that apply

This section includes access to servers, applications and domains in either Cloud1 or Cloud2.

□ **Account Operator:** Members of this group can create, modify and delete accounts for users, groups, and computers located in the Users or Computers containers and organizational units in the domain, except the Domain Controllers. Members of this group do not have permission to modify the Administrator or the Domain Admins groups, nor do they have permission to modify the accounts for members of those groups.

□ **Domain Administrator:** Members of this group have full control of all domain controllers in the domain. By default, the Domain Admins and Enterprise Admins groups are members of the Administrator group. The Administrator account is also a default member.

□ **Local Account:** An account often created for a user that has been added to the local administrator group on a single, specific machine. Local accounts do not have e-mail accounts. With special request and approval, accounts can be added to specific security groups to grant users elevated privileges without elevating the standard user account.

□ **Backup Operator:** Members of this group can back up and restore all files on domain controllers in the domain, regardless of their own individual permissions on those files. Backup operators can also log on to domain controllers and shut them down. This group has no default members.

□ **Print Operator:** Members of this group can manage, create, share, and delete printers connected to domain controllers in the domain. They can also manage Active Directory printer objects in the domain. Members of this group can log on locally to domain controllers in the domain and shut them down.

□ **SUDO Account** – Full access

□ **SUDO Account** – Execute commands

☑ **Other:** Please describe your use case in **Section 4, *Details and Comments***.

2. General Systems — Elevated Access

— Check all that apply

This section includes access to servers, applications and domains in either Cloud1 or Cloud2.

□ **Remote Desktop User for Workstation:** Users of this type can remotely log on to their respective workstation/ laptop in the domain.

□ **Remote Desktop User for Server:** Members of this group can remotely log on to servers in the domain.

□ **Other:** Specific access in addition to standard access that is not considered privileged. Please provide details in **Section 4, *Details and Comments***.

3. Amazon Web Services (AWS) — Privileged Access

— Select one

Per the CFPB AWS Standard Operating Procedures, each account is responsible for managing and deleting resources created by that account, once they are no longer needed, including snapshots (AMIs and EBS), EBS volumes, security groups, instances, objects in S3, etc.

○ **Operations:** Members of this group perform day-to-day operations in AWS such as launching, starting, and stopping instances, creating and deleting snapshots, and monitoring CloudWatch metrics.

○ **DevOps:** Members of this group perform day-to-day operations in AWS such as launching, starting, and stopping instances, creating and deleting snapshots, and monitoring CloudWatch metrics, but only in the DEV VPC.

○ **Power User:** Members of this group perform day-to-day tasks as described in the Operations group, and also make design changes such as creating and deleting subnets, changing security groups and route tables. They can do essentially anything in AWS but do not have write access to IAM policies and do not have access to billing. They can open support tickets.

○ **Administrator:** Members of this group have all the privileges of the Power User group, with two additions: IAM (write access) and Billing (read access). Members of this group create, delete, and modify the permissions of groups and users, and can see Billing info. Membership to this group will be limited to a small number of staff.

○ **Other:** Please describe your use case in **Section 4, *Details and Comments***.

3. Amazon Web Services (AWS) — Elevated Access

— Select one

Per the CFPB AWS Standard Operating Procedures, each account is responsible for managing and deleting resources created by that account, once they are no longer needed, including snapshots (AMIs and EBS), EBS volumes, security groups, instances, objects in S3, etc.

○ **S3 Bucket:** Access to a single S3 bucket from one or more specific locations. Please provide access level, location name, bucket name and other relevant details in Section 4, ***Details and Comments***.

○ **Read-Only Access:** Members of this group can see every aspect of the AWS infrastructure. This is typically used for Cybersecurity personnel and services that perform inventory-related tasks.

○ **Other:** Please describe your use case in **Section 4, *Details and Comments,*** of this form.

4. Details and Comments

— To be completed by Requester

Use the space below to provide details for any of the selections made above in this form. If you are requesting a custom IAM policy, please be sure to include the location(s) from which the access will happen and the specific types of interactions that will take place: specific actions, on which specific resources, subject to which conditions, etc. For assistance crafting a custom IAM policy, please contact Systems Engineering at **`_DL_CFPB_SystemsEngineeringSupport@cfpb.gov`**. *We are happy to help you determine exactly what actions, resources, and conditions are necessary for the work you or your automated tools need to perform. Please add any other information that may be relevant to your request.*

ready only access

5. Requester Certification

I certify by my signature that the information I have provided above is accurate to the best of my knowledge. I have also read, understand, signed and agree to follow the CFPB Privileged Users Rules of Behavior. I am requesting only the level of access required to perform my official duties.

WEI CHEN Digitally signed by WEI CHEN
Date: 2024.05.14 15:37:03
-04'00'

Requester Signature

6. Supervisor Review

— CFPB Supervisor Use Only

I hereby acknowledge that I have reviewed this completed form and validate the need for the level of access requested as being in line with the requester's official duties. I approve only the level of access requested in this form.

MICHAEL GRIFFIN Digitally signed by MICHAEL GRIFFIN
Date: 2024.05.15 06:47:57 -04'00'

Supervisor Signature

7. System Owner Review

— CFPB System Owner Only

I hereby acknowledge that I have reviewed this completed form and validate the need for the level of access requested as being in line with the requester's official duties. I hereby approve only the level of access requested in this form.

Cloud 1 System/Application Owner Signature

Cloud 2 System/Application Owner Signature

Security System/Application Owner Signature

8. Cybersecurity Review

— CFPB Cybersecurity Use Only

The undersigned hereby acknowledge having reviewed this completed form and validated the need for the level of access requested as being in line with the requester's official duties. The undersigned hereby approve only the type of access detailed in this form.

NOTE: *Click the "Not Applicable" checkboxes to remove any signature section that is not required. Each "Not Applicable" box is removed as the corresponding digital signature is applied. This text bar will be removed once all visible signatures are applied.*

□ Not Applicable

Cloud 1 ISSM/ISSO Signature

□ Not Applicable

Cloud 2 ISSM/ISSO Signature

□ Not Applicable

CFPBNet ISSM/ISSO Signature

□ Not Applicable

SalesForce/Third-Party Systems ISSM/ISSO Signature

9. Access Granted

— CFPB Systems Administration Use Only

I confirm that I have granted the system/information access rights requested in this form, as approved by authorized personnel above.

Access Granted Date *(MM/DD/YYYY)*:

Comments:

Cloud1/Cloud2 Application/System Administrator Signature

Access Granted Date *(MM/DD/YYYY)*:

Comments:

Cloud1/Cloud2 Application/System Administrator Signature

Access Granted Date *(MM/DD/YYYY)*:

Comments:

Cloud1/Cloud2 Application/System Administrator Signature

Access Granted Date *(MM/DD/YYYY)*:

Comments:

Cloud1/Cloud2 Application/System Administrator Signature

Access Granted Date *(MM/DD/YYYY)*:

Comments:

Security Application/System Administrator Signature

Access Granted Date *(MM/DD/YYYY)*:

Comments:

Development and Design Application Signature