



Enhanced Direct Enrollment (EDE) Compliance and Audit-Related Frequently Asked Questions (FAQs)

Change History Table

The latest new or updated FAQs are noted in red font.

Version	Date	Summary of Changes
1	3/23/2018	Initial release
2	4/13/2018	- Added subsection "Training" under Section 2 - Added questions 5 and 6 under Section 3 - Added Section 4, "Upstream Entity"
3	5/24/2018	- Added subsection "Security Privacy Assessment Test Plan (SAP)" under Section 2 - Added questions 6 and 7 under Section 2, subsection "Controls" - Added questions 5-7 under Section 5 - Added question 2 under Section 4
4	7/9/2018	- Added question 3 under Section 4 - Added question 8 under Section 5 - Updated questions 6 and 9 under Section 2, subsection 2.2 (Controls) - Added question 2 under Section 3, subsection 3.3 (Business: Other)
5	7/18/2018	- Added question 6 under Section 2, subsection 2.5 (SSP) - Added question 3 under Section 3, subsection 3.2 (Application User Interface) - Added questions 1 and 2 under Section 3, subsection 3.4 (Communications) - Added question 9 under Section 5, (General) - Added question 2 under Section 5, subsection 5.1 (Training)
6	7/26/2018	Added question 2 under Section 3, subsection 3.1 (Audit Process)
7	8/21/2018	- Added questions 5, 6, and 7 under Section 3, subsection 3.3 (Business Other) - Added questions 3 and 4 under Section 4.0 (Upstream Entity FAQs) - Updated question 1 under Section 5, subsection 5.1 (Training)
8	9/17/2018	- Added question 2 under Section 2.0, subsection 2.1 - Added question 3 under Section 3.0, subsection 3.1 - Updated question 6 under Section 3.0, subsection 3.3 - Updated question 3 under Section 4.0 (Upstream Entity FAQs) - Added questions 10, 11, and 12 under Section 5.0
9	10/10/2018	- Updated question 7 under Section 3.0, subsection 3.3 - Updated question 4 under Section 4.0 - Added question 13 under Section 5.0
10	7/12/2019	Added question 14 under Section 5.0
11	8/22/2019	Revised question 14 under Section 5.0

Table of Contents

1.0	Introduction.....	1
2.0	Privacy and Security Audit FAQs	1
2.1	Audit Process	1
2.2	Controls.....	2
2.3	Plan of Action and Milestones.....	10
2.4	Security Privacy Assessment Test Plan	10
2.5	System Security Plan	11
3.0	Business and Application Requirements Audit FAQs.....	12
3.1	Audit Process	12
3.2	Application User Interface.....	16
3.3	Business – Other	16
3.4	Communications Requirements.....	20
4.0	Upstream Entity FAQs.....	22
5.0	General.....	25
5.1	Training.....	36
	Appendix A. Sample Security Design (Adapted by CMS).....	38
	Appendix B. 7 Tips for Building an API-Secure Architecture.....	39

List of Exhibits

Exhibit 1.	CMS High-Risk EDE Controls	5
Exhibit 2.	OWASP Top 10 Application Security Risks, 2017 (1 of 2)	6
Exhibit 3.	OWASP Top 10 Application Security Risks, 2017 (2 of 2)	6
Exhibit 4.	Three-Tier Security Architecture	8
Exhibit 5.	Baseline Versions of Business Audit Documents	14
Exhibit 6.	Upstream Entity Expectations.....	24
Exhibit 7.	Change Categories for Partner-Initiated Changes.....	32



Exhibit 8. Sample Security Design (Adapted by CMS) (Full-size).....	38
---	----

1.0 Introduction

The following frequently asked questions (FAQs) provide further clarification regarding specific audit and program requirements for Enhanced Direct Enrollment (EDE). These FAQs are based on actual questions received from Direct Enrollment (DE) Entities. There are 5 main sections in this document: 1) Introduction, 2) Privacy and Security Audit, 3) Business and Application Requirements Audit, 4) Upstream Entity FAQs, and 5) General. Some sections contain subcategories. Updated and new FAQs are indicated in red type font. The Centers for Medicare & Medicaid Services (CMS), Center for Consumer Information and Insurance Oversight (CCIIO) hopes these FAQs can be of help as DE Entities move forward with EDE. CMS will add additional FAQs in the future.

Note: Some of these FAQs may be outdated. Please refer to the EDE Guidelines (<https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Guidelines-for-Third-party-Auditors-EDE-PY19PY20.pdf>) for the most up-to-date information.

2.0 Privacy and Security Audit FAQs

2.1 Audit Process

- 1. Where can DE Entities find information about the privacy and security audit? What documentation/information can DE Entities provide to their auditor to help them estimate audit requirements and level of effort (LOE)?**
 - The EDE Auditor Guidelines contain information about the privacy and security audit requirements. The privacy and security audit templates, as well as the list of 292 security and privacy controls, are located on CMSzONE at the following link: <https://zone.cms.gov/document/enhanced-direct-enrollment-edo-documents-and-materials>. (Note that DE Entities must set up a CMS Enterprise Portal account and request zONE access to view the zONE website.)
 - The Privacy/Security Standards training module will also review the privacy and security audit requirements; CMS expects that the Privacy/Security Standards training module will be available soon.
- 2. Can DE Entities and Auditors complete security and privacy testing and audit activities within a testing or production environment?**
 - CMS recommends that EDE Partners should have separate test and/or preproduction environments hosting an instance of the production operational environment. They should mirror one another to create an accurate response to changes as they are made for testing.

Systems can be tested in pre-production environments as long as these environments mirror the production environment. Deviations should be properly documented.

- CMS recommends that all security and privacy audit activities include verification and validation of vulnerabilities (findings) and continue to be performed within the pre-production environment. EDE Partners will certify and attest to the fact that all system vulnerabilities, found as a result of security and privacy audits performed in a pre-production environment, will also be mitigated in the production environment.

2.2 Controls¹

1. **There are a handful of National Institute of Standards and Technology (NIST) controls that were required for the DE Proxy (DEP) program, but which are NOT required for the EDE program (according to the “streamlined list” of controls that DE Entities were provided). From a CMS perspective, do DE Entities need to continue to implement/maintain those controls, which are no longer listed as required? For reference, those controls are: 1) NIST Control Title, AC-3(9) Access Enforcement: Controlled Release, 2) IA-5(15) Authenticator Management: FICAM-Approved Products and Services, 3) PE-18 Location of Information System Components, and 4) TR-2 System of Records Notices and Privacy Act.**
 - No, partners do not need to specifically maintain the DEP controls. The EDE control set supersedes the DEP control set. While some of the control elements may have been merged with the EDE controls, partners no longer need to implement or maintain the DEP controls.
2. **Regarding AU-10, “Non-repudiation,” is this part of our expected Public Key Infrastructure (PKI) implementation? Are there specific actions for which CMS would like us to ensure non-repudiation?**
 - Yes, PKI digital signature and certificate would address non-repudiation. Non-repudiation is a critical element of accountability and accuracy of information in system history and logs, and it is important for investigating incidents and breaches. Please ensure system history and logs are protected and not being tampered with or altered.
3. **Are the 292 EDE security/privacy controls final? Are there any changes that can be made to the associated CMS templates? Alternatively, can Federal Risk and Authorization Management Program (FedRAMP) templates be substituted?**
 - The security/privacy controls rolled out in early December 2017 are final. However, CMS released updated security and privacy templates on March 6, 2018; they are available on the [CMS zONE EDE page](#). CMS may occasionally make small minor revisions to account for

¹ The EDE security and privacy controls can be reviewed in the SSP workbook on the [CMS zONE EDE page](#).

minor corrections or discrepancies; CMS will note changes.) DE Entities must use those templates and cannot substitute the FedRAMP templates.

- Note that the FedRAMP controls were designed for Entities providing Cloud services to the Federal Government (i.e., the “skinny” control set is due to the fact that the Federal Entity is then responsible for the remaining controls dictated by its agency). Keep in mind these controls are also required based on CMS’ agreements with our federal partners, which connect via the Data Services Hub (Internal Revenue Service, Social Security Administration, etc.)
- 4. We are worried about the timeline to pass all the security/privacy requirements. Can CMS advise on which controls to prioritize?**
- See question #6 added on 5/24/18 (“Are there any security and privacy controls that must be remediated prior to submitting the Security and Privacy Assessment Report (SAR) and Plan of Action and Milestones (POA&M)?”) and Exhibit 1.
 - CMS encourages partners to do their best to submit the security/privacy templates as soon as possible this summer, so CMS can help each partner go live with EDE in production before the testing and ramp-up to Open Enrollment begins. However, in parallel, CMS is also working on shoring up additional resources to expedite CMS’ review of each DE partners’ audit findings to avoid bottlenecking for partners who are not ready until the fall of 2018.
 - It is important that partners demonstrate compliance with all 292 controls. CMS recommends that partners first prioritize compliance with operational controls. However; it is still important that partners show compliance with administrative controls. (A partner that simply ignores the documentation controls or that has numerous findings in this area would likely not be approved for EDE.)
 - In general, CMS understands that any given partner may not have all its solutions in place; in those cases, the partner should clearly document a solid plan and timeframe on how it will meet missing components (barring any critical controls) before the plan year 2019 OEP. Critical controls can be reviewed at www.CISecurity.org; however, please note that CMS considers all the controls as essential.
- 5. Can CMS provide additional guidance around the control enhancement AU-6(3), “Audit Review, Analysis, and Reporting | Correlate Audit Repositories?” Is there any detailed guidance on formats “compliant with Federal (e.g., Continuous Diagnostics and Mitigation) requirements?”**
- See NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*. The audit logs are sent in a raw, unedited format so that queries can be made on the data by the analytic tools. This provides assurance that logs

have not been altered to remove any evidence of tampering or malicious activity. The raw format is going to be dependent on the automated tools in use by the partner. For example, audit records can be sent directly to SPLUNK and your Continuous Diagnostic Monitoring (CDM) team would use the tools within SPLUNK to query the content and create alerts and monitoring reports. If the logs were converted to an incompatible format prior to submission, the CDM team would not be able to analyze the data.

- It is understandable that there may not be a separate CDM team in the organization. This control is just to provide assurance that the data collected are the data reviewed by the CDM team (which could be the same team that is responsible for the system security operations.)

6. Are there any security and privacy controls that must be remediated prior to submitting the SAR and POA&M?

- CMS considers all 292 controls in the EDE System Security and Privacy Plan (SSP) to be critical and the controls were carefully selected for that reason. However, CMS is providing a list of controls that are considered HIGH risk if not fully implemented (see Exhibit 1) as a courtesy to help DE Entities prioritize remediation and level-set expectations.
- Auditors may indicate high-risk findings, in which cases CMS will reconcile an auditor's risk categorization with what CMS considers critical. When CMS reviews the DE Entity's privacy and security audit findings, CMS will also indicate which controls must be expedited for remediation.
- CMS expects that DE Entities will try to try to implement 100% of the 292 controls; failing that, DE Entities should not submit a POA&M with any high-risk findings that have not been remediated. Implementing 90% of the controls is not a "gold standard," but a DE Entity's chances for success are better. Depending on the number, severity, and potential impacts, failing only 10% of the controls does not guarantee success. For example, failing 29 of the 39 Access Controls or all Systems and Communications Protection Controls would present a risk to CMS. Failing to complete control families without any high-risk controls would be problematic.
- CMS is looking at the overall security posture of the DE Entity and its ability to maintain that posture. Focusing only on the high-risk controls does not present a stable security posture, similar to presenting a report containing any high-risk findings. Trying to meet the minimum standards is not a laudable goal and would be obvious to the team reviewing the reports.
- Furthermore, this guidance does not imply that a POA&M submission with only MODERATE risk findings will be automatically approved. CMS foresees some scenarios where a combination of multiple moderate risk findings would constitute a high risk to CMS when presented in aggregate. See Exhibit 1 for the list of high-risk privacy and security controls.

Exhibit 1. CMS High-Risk EDE Controls

Control #	Security/Privacy Control Name
AC-7	Unsuccessful Logon Attempts
AC-11	Session Lock
AC-12	Session Termination
AC-14	Permitted Actions Without Identification or Authentication
AT-2	Security Awareness Training
AU-2	Audit Events
AU-6	Audit Review, Analysis, and Reporting
AU-9	Protection of Audit Information
CA-2	Security Assessments
CA-5	Plan of Action and Milestones
CA-8(1)	Independent Penetration Agent
CM-2	Baseline Configuration
CM-6	Configuration Settings
IA-2	Identification and Authentication (Organizational Users)
IA-4	Identifier Management
IA-5	Authenticator Management
IA-5(1)	Password-Based Authentication
IA-8	Identification and Authentication (Non-Organizational Users)
IA-8(2)	Acceptance of Third-Party Credentials
IR-4	Incident Handling
IR-5	Incident Monitoring
IR-6	Incident Reporting
MA-3(2)	Inspect Media
PL-2	System Security Plan
PS-3	Personnel Screening
RA-3	Risk Assessment
SC-23	Session Authenticity
SI-10	Information Input Validation
SI-11	Error Handling
AR-2	Privacy Impact and Privacy Program
AR-8	Accounting of Disclosures
DM-3	Minimization of PII Used in Testing, Training, and Research
DM-3 (1)	Minimization of PII Used in Testing, Training, and Research/Risk Minimization Techniques
IP-1	Consent
IP-2	Individual Access
SE-2	Privacy Incident Response

Below, Exhibit 2 and Exhibit 3 provide additional information on application security risks from the Open Web Application Security Project (OWASP).

T10 OWASP Top 10 Application Security Risks –2017	
A1:2017 Injection	Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
A2:2017 Broken Authentication	Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities (temporarily or permanently).
A3:2017 Sensitive Data Exposure	Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.
A4:2017 XML External Entity (XXE)	Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal SMB file shares on unpatched Windows servers, internal port scanning, remote code execution, and denial of service attacks, such as the Billion Laughs attack.
A5:2017 Broken Access Control	Restrictions on what authenticated users are allowed to do are not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.

Exhibit 2. OWASP Top 10 Application Security Risks, 2017 (1 of 2)

T10 OWASP Top 10 Application Security Risks –2017	
A6:2017 Security Misconfiguration	Security misconfiguration is the most common issue in the data, which is due in part to manual or ad hoc configuration (or not configuring at all), insecure default configurations, open S3 buckets, misconfigured HTTP headers, error messages containing sensitive information, not patching or upgrading systems, frameworks, dependencies, and components in a timely fashion (or at all).
A7:2017 Cross-Site Scripting (XSS)	XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user supplied data using a browser API that can create JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
A8:2017 Insecure Deserialization	Insecure deserialization flaws occur when an application receives hostile serialized objects. Insecure deserialization leads to remote code execution. Even if deserialization flaws do not result in remote code execution, serialized objects can be replayed, tampered or deleted to spoof users, conduct injection attacks, and elevate privileges.
A9:2017 Using Components with Known Vulnerabilities	Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.
A10:2017 Insufficient Logging & Monitoring	Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

Exhibit 3. OWASP Top 10 Application Security Risks, 2017 (2 of 2)

7. Is the auditor only required to list controls that are in the SSP?

INFORMATION NOT RELEASABLE TO THE PUBLIC UNLESS AUTHORIZED BY LAW: This information has not been publicly disclosed and may be privileged and confidential. It is for internal government use only and must not be disseminated, distributed, or copied to persons not authorized to receive the information. Unauthorized disclosure may result in prosecution to the full extent of the law.

- Correct, for the EDE authorization, CMS is not concerned about controls outside of the ones included in the SSP.
- 8. **Does CMS only want to see documentation of failed security and privacy controls? Is there anywhere the auditor can document controls that are compliant?**
 - There is no restriction on what the auditor can document. The assumption is that if the auditor only shows failures, then everything else passed, but if the auditor is traditionally reporting controls that passed as well, that is fine.
 - The auditor may document implementation for controls that are both compliant and non-compliant.
- 9. **Are there any guidelines or parameters that an EDE Partner's system boundaries or architecture must follow? Are there technical resources EDE partners can reference that provide guidance on securing systems?**
 - If systems reside on the same subnet, there is a chance they can comeingle with each other; in that case, they must be included in the DE Entity's boundary. If there is a firewall between the system and the subnet, then, an auditor would only need to look at the firewall to make sure that a security threat could not come across and reach CMS. CMS is concerned with anything that can reach CMS through your network.
 - CMS adapted the "Three-Tier Architecture Model" from the Microsoft® Development Center available here: [https://msdn.microsoft.com/en-us/library/windows/desktop/ms685068\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/ms685068(v=vs.85).aspx)

The three-tier architecture model, which is the fundamental framework for the logical design model, segments an application's components into three tiers of services. These tiers do not necessarily correspond to physical locations on various computers on a network, but rather to logical layers of the application. How the pieces of an application are distributed in a physical topology can change, depending on the system requirements.
 - The three-tier architecture model is pictured below in Exhibit 4.

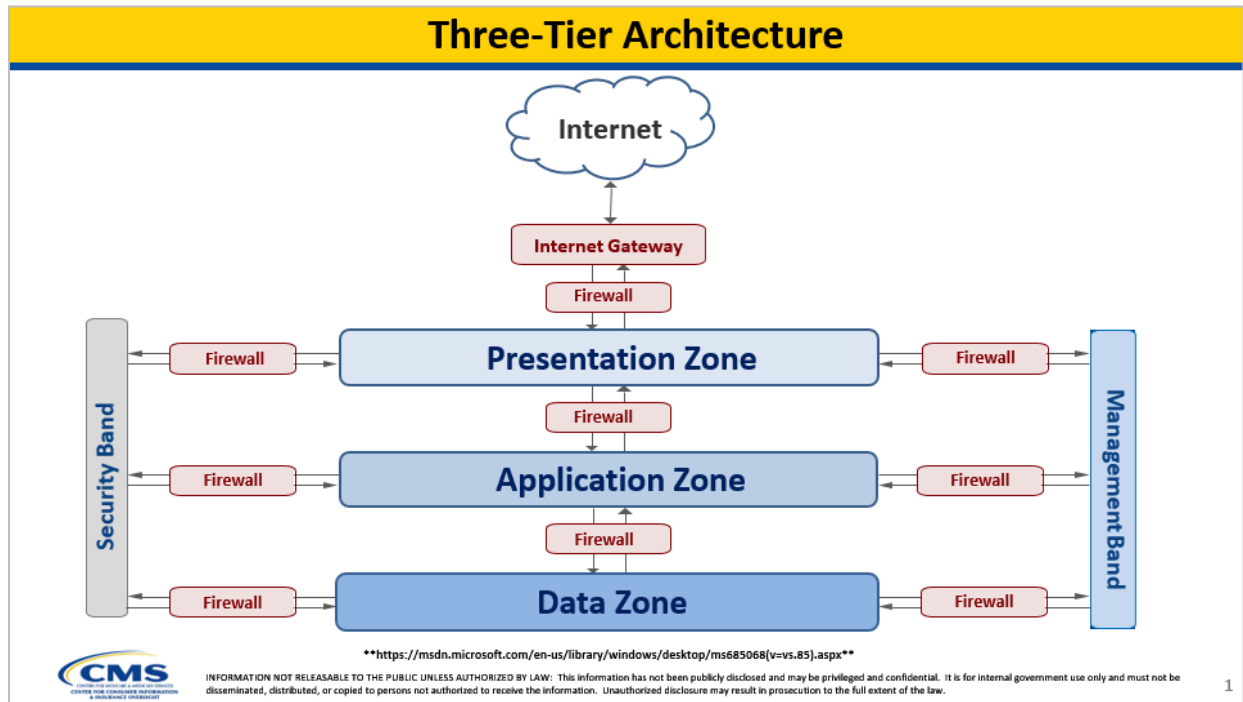


Exhibit 4. Three-Tier Security Architecture²

See **Appendix A** for a sample security design.

- Following are brief descriptions of the services that the Microsoft's three-tier architecture model allocates to each tier.³

The presentation tier, or user services layer, gives a user access to the application. This layer presents data to the user and optionally permits data manipulation and data entry. The two main types of user interface for this layer are the traditional application and the Web-based application. Web-based applications now often contain most of the data manipulation features that traditional applications use. This is accomplished through use of Dynamic HTML and client-side data sources and data cursors.

Note: *In a three-tiered application, the client-side application will be skinnier than a client-server application because it will not contain the service*

² Adapted by CMS from [Using a Three-Tier Architecture Model webpage](#)

³ Microsoft. (2018, May 31). Using a Three-tier Architecture Model. Retrieved from <https://docs.microsoft.com/en-us/windows/desktop/cosstdk/using-a-three-tier-architecture-model>

components now located in the middle tier. This results in less overhead for the user, but more network traffic for the system because components are distributed among different machines.

The middle tier, or business services layer, consists of business and data rules. Also referred to as the business logic tier, the middle tier is where COM+ developers can solve mission-critical business problems and achieve major productivity advantages. The components that make up this layer can exist on a server machine, to assist in resource sharing. These components can be used to enforce business rules, such as business algorithms and legal or governmental regulations, and data rules, which are designed to keep the data structures consistent within either specific or multiple databases. Because these middle-tier components are not tied to a specific client, they can be used by all applications and can be moved to different locations, as response time and other rules require. For example, simple edits can be placed on the client side to minimize network round-trips, or data rules can be placed in stored procedures.

The data tier, or data services layer, interacts with persistent data usually stored in a database or in permanent storage. This is the actual DBMS access layer. It can be accessed through the business services layer and on occasion by the user services layer. This layer consists of data access components (rather than raw DBMS connections) to aid in resource sharing and to allow clients to be configured without installing the DBMS libraries and ODBC drivers on each client.

During an application's life cycle, the three-tier approach provides benefits like reusability, flexibility, manageability, maintainability, and scalability. You can share and reuse the components and services you create, and you can distribute them across a network of computers as needed. You can divide large and complex projects into simpler projects and assign them to different programmers or programming teams. You can also deploy components and services on a server to help keep up with changes, and you can redeploy them as growth of the application's user base, data, and transaction volume increases.⁴

10. In reference to the AC-4 (Information Flow Enforcement); SC-2 (Application Partitioning), and SC-7 (Boundary Protection): For applications that are part of a larger enterprise, can a user process be stored or processed to or from a non-EDE

⁴ In Appendix B, CMS has provided seven key best practices to consider when designing the secure architecture needed to implement a trusted API gateway. The seven key best practices document is also enclosed as a PDF as a zip file.

application? Can the applications remain in the DE Entity’s enterprise environment or does CMS require the applications be separated out? If the DE Entity would like for applications to stay part of their enterprise environment, can they stay?

- CMS highly recommends that applications be segregated.
- If enterprise shared services are co-mingled with EDE applications, then all co-mingled enterprise shared services must be part of the security audit boundary.
- CMS understands there are limitations and that DE Entities likely cannot buy new equipment. Applications and user processes can live in the same environment.
- While it is highly recommended that EDE applications be segregated from the DE Entity’s enterprise environment, EDE applications can be part of the DE Entity’s existing enterprise environment. However, the existing enterprise environment should be part of the EDE boundary and be audited.

2.3 Plan of Action and Milestones

1. In the provided CMS Plan of Action and Milestones (POA&M) template, the NIST controls have been “filled in” where there are organization-defined parameters. Do partners need to use the parameters that have been filled in, or can we replace them with our own organization-specific parameters as indicated by the NIST 800-53 Rev. 4 control language?

- The NIST documentation is written to allow a federal agency to define the implementation standard based on its security requirements. CMS Enterprise Security replaced the “agency defined” notation with the standards that the CMS Chief Information Security Officer (CISO) requires for all FISMA applications operating on the CMS network. CMS has taken the standards defined by CMS and used those in the SSP Workbook. The standards defined in the SSP Workbook are the ones that partners must implement.

2.4 Security Privacy Assessment Test Plan

1. Is the third-party auditor required to use the CMS Security and Privacy Controls Assessment Test Plan (SAP) or may it use its own Test Plan template?

- The DE Entity and its third-party auditor must jointly complete and agree to a SAP before the start of the Security and Privacy assessment. The auditor may use either the CMS SAP Template or its own Test Plan template. If the auditor chooses to use its own Test Plan template, the DE Entity must remind the auditor that the template must have all the elements contained in the CMS-provided SAP template. If elements are missing from the auditor’s template, there is a risk that these elements will not be tested and reported to CMS in the SAR. For that reason, CMS highly recommends the use of the CMS SAP Template to ensure

that all the required elements are assessed and presented in a manner that will facilitate the CMS review and adjudication of each request to connect.

- **Please Note:** The DE Entity is **not** required to submit the completed SAP to CMS.
- 2. **Appendix A (“Test Case Procedures and Results”) in the Security and Privacy Controls Assessment Test Plan states “Results of the security and privacy control test case procedures shall be recorded and must be attached.” Is there a template available for Appendix A?**
- Security and Privacy Assessment results must be recorded and provided to CMS in the SAR. The SAR template is available on CMS zONE at the following link:
<https://zone.cms.gov/document/enhanced-direct-enrollment-edo-documents-and-materials>

2.5 System Security Plan⁵

1. **(In reference to SSP workbook section 7, Information System Type) The System Security Plan (SSP) workbook says “This section is to be used only for Non-Exchange Entities (NEEs) that have systems or a portion of their systems operating in a cloud environment. The <Information System Abbreviation> makes use of unique managed service provider architecture layer(s).” If the NEE does not have systems or a portion of its systems operating in a cloud environment, how does CMS want the NEE to respond? Should the NEE just mark that section as “Not Applicable?”**
- Yes, please respond that the NEE does not use a hosted cloud environment.
2. **(In reference to SSP workbook section 14, Systems Security Plan Attachments) Since the instruction says the documents “should” be developed and maintained, are these attachments required or merely recommended?**
- CMS requires that the NEE has these documents and supplies them to an independent third-party assessor for review. Failing to provide these documents for review would be a finding documented in the final Security and Privacy Assessment Report (SAR).
3. **Table 14-7 (“Required Security and Privacy Agreements and Compliance Artifacts”) in the SSP lists several artifacts that are not required to be delivered to CMS. In that case, is it correct to assume that those documents need only to be made available to the assessor for the assessor to complete their assessment?**
- Yes, that is correct. The independent third-party auditor must review the documents listed in Table 14-7. The SAP will provide a list of documents for review by the auditor. The auditor may choose to use its own Test Plan template and the Partner should remind the auditor that

⁵ The SSP workbook for EDE is available on the [CMS zONE EDE page](#).

the auditor's template must have all the elements contained in the CMS-provided SAP template. The SAP and SAR are linked and if elements are missing from the auditor's template, there is a risk that these elements will not be tested and reported to CMS in the SAR.

4. **In SSP section 13 - AC-17 (1), Automated Monitoring/Control, what are “distributed blocking rules” and where might one find a list of “industry best practice” ones? A Google search on “distributed blocking rules” yields only two results, both of which point to CMS documents that provide no further clarity.**
 - CMS, Department of Homeland Security (DHS), United States Computer Emergency Readiness Team (US-CERT), or commercial organizations may have a mechanism to issue/distribute lists of IP addresses, ports, or services that organizations receive to block at their remote access points based on the latest threats and cyber-attacks. When this happens, the organization should implement these blocking rules within one hour of receipt.
5. **Do the consumer accounts created by the DE Entity for access to the DE Entity system need to be Federal Identity, Credential and Access Management (FICAM)-compliant?**
 - Per IA-8(2) in the SSP Workbook, only use FICAM-approved credentials when connecting to CMS.
6. **In the SSP workbook, can the control implementation description refer to the DE Entity's procedures for the control or does the DE Entity need to copy and paste the language from its procedures into the SSP workbook?**
 - CMS recommends pasting the procedure into the SSP workbook. If DE Entities provide a reference, then they would have to provide the procedure to the auditor. CMS recommends spelling out the procedure within the SSP workbook.

3.0 Business and Application Requirements Audit FAQs

3.1 Audit Process

1. **When will CCIIO provide more information on the business audit requirements? What documentation/information can I provide to my business auditor to help them estimate audit requirements and level of effort?**
 - The Guidelines for Third-party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment Pathway and Related Oversight Requirements (EDE Auditor Guidelines) published by CMS on February 22, 2018 (<https://www.cms.gov/CCIIO/index.html>) contain information about the business audit requirements. CCIIO will also release multiple toolkits that will contain templates the auditor must use to verify the DE Entity's compliance with business audit requirements. The requirements that comprise the most significant portion of

the business audit requirements are available in the Federally-facilitated Exchange (FFE) User Interface (UI) Application Principles (FFE UI Application Principles) document located on CMS zONE at the following link: <https://zone.cms.gov/document/enhanced-direct-enrollment-edo-documents-and-materials>. (Note that DE entities must have a CMS Enterprise Portal account to access the FFE UI Principles document.)

- Update: CMS has since released all business audit toolkits and templates in a zip file on CMS zONE at the link above.
- 2. **Does CMS have any guidance for using the updated Business Requirements Audit Report Template and toolkits once we have begun the business requirements audit?**
 - As previously messaged, the Business Requirements Audit Report Template and accompanying toolkits are subject to change. CMS has revised several of these documents since they were initially released. Effective July 26, 2018, CMS will require DE Entities and their Auditors to use the revised template and toolkit versions as set forth in this FAQ.
 - CMS has established a "baseline" version of the Business Requirements Audit Report Template and each accompanying toolkit. These baseline versions include all of CMS' revisions through July 5, 2018. **Auditors must use the baseline version—or a version released after the baseline version**—of the Business Requirements Audit Report Template and each accompanying toolkit to conduct the business requirements audit.
 - Exhibit 5 below indicates the document name and file date of the baseline version of the Business Requirements Audit Report Template and each toolkit.

Exhibit 5. Baseline Versions of Business Audit Documents

Toolkit	Document Name of Baseline Version	Date of Baseline Version
API Functional Integration Toolkit	API_Functional_Integration_Toolkit_05152018.xlsx	The file is dated 5/15/2018
Communications Toolkit	Communications Toolkit_06112018.xlsx	The file is dated 6/11/2018
Application User Interface (UI) Toolkit	Application UI Toolkit_07032018.xlsx	The file is dated 7/3/2018
Eligibility Results Toolkit(s)	EDE_Eligibility Results Toolkit_Phase 1_07022018.xlsx EDE_Eligibility Results Toolkit_Phase 2_07022018.xlsx EDE_Eligibility Results Toolkit_Phase 3_07022018.xlsx	The files are dated 7/2/2018
EDE Business Audit Instructions and Report Template	EDE Business Audit Instructions and Report Template_07052018.docx	The file is dated 7/5/2018

How to Use the Baseline Toolkits

- If Auditors have started recording findings in previous toolkit versions, they must transfer findings from previous toolkit versions into the baseline versions of the toolkits. For example, if an Auditor has started documenting findings in the Application UI Toolkit released on 5/11/2018, it must transfer its findings into the baseline version of the toolkit dated 7/3/2018.
- Auditors must also review the baseline toolkit revisions to assess if they need to re-review requirements before transferring their findings. Auditors must review all toolkit revisions published through 7/5/2018. These revisions are noted in different colored fonts in the baseline toolkit; each toolkit has a revision key on either the DE Entity User Guide tab or the Auditor User Guide tab.
- For example, in the example described above, the Auditor would need to review all revisions made between the version released on 5/21/2018 (initial version) and the 7/3/2018 baseline version in the Application UI toolkit, which are noted in colored fonts in the baseline version of the Application UI Toolkit (i.e., purple font indicates revisions made on 5/22/2018 and green font indicates revisions made on 7/3/2018) before transferring its original findings to the baseline version. If, during its review of the revisions, the Auditor determines re-review of a requirement is necessary, it should re-review that requirement and record its updated findings in the baseline toolkit.
- Additionally, Auditors must not change existing font colors; Auditors may use black font to document their findings but must not document their findings in another font color that is already used within the toolkits.

How to Use Future Toolkit Versions

- CMS may publish future revised versions of the toolkits. Auditors may use forthcoming toolkit versions, instead of the baseline versions, but are not required to use any versions released after the baseline version (see below for additional information). DE Entities must confirm that their Auditors used either:
 - The baseline version of each toolkit, **OR**
 - A toolkit version published after the baseline version for each toolkit.
- When DE Entities submit the toolkits to CMS, they must send an accompanying email to the DE help desk that notes which toolkit versions their Auditor used.

Change Request Process

- CMS may require DE Entities to implement certain revisions released in future toolkit versions. However, CMS will give DE Entities the option to implement required revisions by submitting supplemental documentation instead of submitting the version of the toolkit containing the revision(s). Required revisions (i.e., toolkit revisions that DE Entities must implement) will be considered CMS-initiated change requests (CRs). Information about the CMS-initiated CR process is forthcoming. These CMS-initiated CRs can be included as part of the business requirements audit, but CMS will issue a separate process and provide a timeline for DE Entities to implement the changes (see “What is the CMS-Initiated Change Request Process for DE Entities Using EDE in Plan Year 2019?” under Section 5.0).

3. Can DE Entities use automated translation tools to translate the eligibility application in Spanish?

- An Auditor must independently confirm that the Spanish-language version of the application and critical communications have the same meaning as the English-language version before CMS will permit a DE Entity to operate an EDE pathway in Texas.
- See the Frequently Asked Questions (FAQs) Regarding Spanish Translation and Audit Requirements for Enhanced Direct Enrollment (EDE) Entities Serving Consumers in States with Federally-facilitated Exchanges (FFE)s.
- DE Entities may use automated translation tools, however, a DE Entity's use of an automated translation tool to translate the application and critical communications from English to Spanish alone is not sufficient to satisfy the Non-English-language Version of the Application UI and Communication Materials requirement.
- If a DE Entity uses an automated translation tool, the Auditor must still meet the audit standard defined in the first bullet above.

- In general, CMS recommends against the use of automated translation tools as a standalone solution by DE entities. When automated translation tools are used, the proper context of the language is often lost and the language, tone, and regional dialect of the translated content can be inconsistent.

3.2 Application User Interface

1. **In the UI Companion Guide, are there specific requirements for the Application Summary that is displayed when consumers attest and sign the application? What are the requirements that the auditor will hold us to for this?**
 - The requirements for the application summary are included in columns M, N, and O for the application review row (row 241) in the UI Questions tab within the UI Companion Guide spreadsheet which is embedded within the FFE UI Application Principles document on zONE. CMS will make periodic updates to his document.
2. **There are upcoming changes, such as Qualified Small Employer Health Reimbursement Arrangement (QSEHRA) changes, that will take place in the summer after the initial EDE go-live dates. Will CMS have guidelines regarding turnaround time for updates such as this one, to ensure we are compliant with any changes made by CMS?**
 - Anytime there are CMS-initiated application changes after partners go live, CMS will provide timeline requirements for partner implementation. Timeline requirements are unique to the application update and CMS will provide application content and requirements for each update. For QSEHRA application updates, any partners that have already gone live will be given guidance on the timing expectations for updating their application.
3. **When a consumer requests an additional Medicaid determination from the states, is there any special handling? Are there any requirements around what to display as confirmation to the consumer?**
 - There is no special handling required; however, once the consumer makes the request, the UI should indicate that the consumer has made the request (e.g., it should be greyed out). The consumer should know that its information is being sent to the state.

3.3 Business – Other

1. **In Section II.D of the EDE Auditor Guidelines, the last paragraph speaks to the DE Entity being responsible for ensuring its agents and brokers comply with the terms and conditions set forth in the EDE Agreement. As agents and brokers do not have to sign an agreement themselves, what is CMS' expectation here with regards to how the DE Entity would ensure this compliance?**

- CMS anticipates that a DE Entity’s pathway will contain sufficient safeguards and policies and procedures to protect against noncompliance with respect to the EDE Agreement by any authorized, downstream agents and brokers who are using the EDE pathway or interacting or managing any consumer applications associated with the EDE pathway. For example, CMS does not require downstream agents or brokers to comply with all privacy and security requirements of the Interconnection Security Agreement (ISA) independently; however, a compliant EDE pathway managed by the DE Entity should protect against noncompliant use of the pathway by said agent or broker with respect to the privacy and security standards.
- 2. Does CMS have any guidance regarding marketing of ancillary products for DE Entities?**
- CMS has shared guidance on marketing ancillary products zONE in the following places:
 - Web-broker Community (Web-broker Guidance and FAQs page:
<https://zone.cms.gov/document/web-broker-guidance-and-frequently-asked-question-faq-documents>)
 - Issuer Community (DE Documents and Materials page:
<https://zone.cms.gov/document/direct-enrollment-de-documents-and-materials>)
 - CMS considers the marketing of ancillary regulated dental and vision insurance products after assisting consumers with their QHP selections to be consistent with CMS guidance from 2016 and the most recent Enrollment Manual.
 - CMS also considers including QHPs and ancillary regulated dental and vision insurance products in a common “shopping cart” to be consistent with prior guidance, as long as the websites make clear that advance payments of the premium tax credit (APTC) and/or cost sharing reductions (CSRs) consumers are eligible for apply only to QHPs offered through the Exchange.
- 3. What is CMS’ stance for those documents and artifacts DE entities submit to it and/or the auditors with regards to state freedom of information or sunshine laws?**
- CMS does not have a position on state law. DE entities and qualified health plan (QHP) issuers must comply with applicable state law.
- 4. The review standard for the “Section 508-compliant user interface (UI)” business Operational Readiness Review (ORR) review category states “The Auditor must confirm that the DE Entity’s application meets the requirements set forth under Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. § 749(d)).” Are there any reference materials an auditor may use to verify that the DE Entity’s application UI is 508-compliant?**

- There are several resources auditors can use. The following are 508 compliance resources provided by the General Services Administration (GSA) on the <https://section508.gov/website>:
 - **Creating Accessible Digital Products:** <https://section508.gov/create>
 - **Developing Accessible Digital Products:** <https://section508.gov/create/web-content>
 - **Testing Accessible Digital Products and Methods:** <https://section508.gov/test>
- The United States Access Board’s website provides information about the revised 508 standards from 2017: <https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-ict-refresh/final-rule/text-of-the-standards-and-guidelines>
 - The Web Accessibility Initiative developed the *Web Content Accessibility Guidelines*, which are available here: <https://www.w3.org/WAI/standards-guidelines/wcag/>

5. Does adding content to the application UI require a UI consultation with CMS?

- Generally, content added to the application UI experience must fall within the bounds of the requirements identified in the FFE UI Application Principles document and Application UI Toolkit for each particular question, including any accompanying informational or question assistance text.
- These documents can be accessed at the following link on CMSzONE: <https://zone.cms.gov/document/enhanced-direct-enrollment-edc-documents-and-materials>
- While not required, if a DE Entity is planning on making any customizations to the application questions or flow that is not very clearly within the guardrails laid out in the FFE UI Application Principles or Application UI Toolkit, it is strongly encouraged that DE Entities request (via the DE Help Desk) a UI consult with CMS.
- CMS also encourages DE Entities to request a UI consult sooner than later (i.e. leverage resources available now that may not be as available during peak EDE audit submissions) and well in advance of submitting business audit findings.
- Disclaimer: The UI consult does not replace the audit findings. CMS needs independent verification that the question implemented in the application works as detailed in the Toolkit. CMS incorporates UI consultation feedback when updating the toolkits.

6. With respect to the Section 508 compliance requirement for the business audit, does CMS require additional documentation to show that the DE Entity’s application UI is Section 508-compliant? If so, what is considered sufficient documentation?

- CMS does not require that auditors complete a specific report or include other supplemental documentation that confirms compliance with the Section 508 compliance requirement. Within the Business Requirements Audit Report Template, the Auditor must confirm that the DE Entity's application UI is Section-508 compliant.
- If the Auditor has test results from running a 508-compliance test, it can use the information from the test report to populate the Business Requirements Audit Report Template.
- If a DE Entity uses a 508 compliance testing tool to verify that its UI is 508-compliant, its Auditor must, at a minimum, review the results produced by the testing tool and document any non-compliance, as well as any mitigation or remediation to address the non-compliance.
 - It is not sufficient for an Auditor to state that a DE Entity complies with the 508-Compliant UI requirement by confirming that the DE Entity utilized a 508 compliance testing tool.
- It is acceptable for a DE Entity's audit to document compliance with Web Content Applicability Guidelines (WCAG) 2.0 AA to satisfy the Section 508-Compliant UI requirement.
 - The revised 508 standards reference the WCAG standards. Please see the following resource for an example: <https://www.section508.gov/create/applicability-conformance>.
 - The Auditor should include a note within the audit explaining that the revised Section 508 requirements specify WCAG 2.0 AA.

7. What are the Spanish translation and audit documentation requirements?

- When applicable, the *EDE Business Audit Instructions and Report Template* requires Auditors to document compliance with the “Non-English-language Version of the Application UI and Communication Materials” requirement within the Business Requirements Audit Report Template as well as within the Application UI and Communications toolkits. Specifically, Auditors have two options for how they may document compliance within the toolkits:
 - the Auditor can add additional columns for the auditor compliance findings fields (yellow-shaded columns) to the Application UI and Communications toolkits to document compliance of the Spanish-language translation, or
 - the Auditor can complete the Spanish audit in a second copy of the Application UI and Communications toolkits as a supplemental submission after the initial ORR submission.

- CMS provided additional guidance related to translation and communications requirements in an FAQ posted to CCIIO's website (<https://www.cms.gov/CCIIO/Programs-and-Initiatives/Health-Insurance-Marketplaces/Downloads/FAQ-EDE-Spanish-Translation-and-Audit-Requirements.PDF>).
 - CMS requests that Auditors document compliance with the “Non-English-language Version of the Application UI and Communication Materials” requirement in accordance with one of the two methods described above.
 - *Clarification:* When applicable, DE Entities offering EDE are required to translate website pages (e.g., the application UI) into Spanish on consumer-facing websites.
 - DE Entities are not required to translate the UI on agent/broker-facing websites.
- 8. What are the new User ID and agent/broker requirements for primary entities using EDE that were announced in November 2018?**
- Primary EDE Partners will need to submit the following to demonstrate they have made the appropriate system and procedure updates:
 - **Written attestation**
 - Note: this must be a written attestation that you are compliant with requirements communicated by CMS. Please restate your understanding of your responsibility. CMS is not providing template language; CMS requests that you develop a letter on company letterhead, have it signed by someone in your organization that has the legal authority to sign a statement of this nature, and then return a scanned copy via the secure portal.
 - **Policies and procedures** document for implementing the new process
 - **Desktop flow** (e.g., Agent/Broker verification)
 - All documents should be submitted to CMS via the secure portal. Please contact the DE Help Desk (directenrollment@cms.hhs.gov) if you do not already have secure portal access.

3.4 Communications Requirements

- 1. What are the requirements for EDE Partners, in terms of notifying consumers when new notices become available? Do EDE Partners need to run daily batch processes to check the Metadata Search application programming interface (API) for new notices?**
- For this year, CMS will not be implementing push notifications for EDE, and will therefore not require partners to send consumers email notifications when new notices become

available. EDE partners are required to inform consumers they will continue to receive additional communications from HealthCare.gov. However, EDE partners should encourage consumers to return to the DE Partner site rather than HealthCare.gov to address their needs. EDE partners should strongly consider embedding this information into the initial Application Submission communication (e.g., “Be aware you may get e-mails from HealthCare.gov but come back to us for all of your needs”).

- Partners are required to make the Eligibility Determination Notice (EDN) available to the consumer in the UI upon application submission. Post-application submission, partners must make all consumer notices available to the consumer within their UI. Furthermore, when a consumer leaves and later returns to a partner’s site, the partner should refresh the notices displayed to the consumer within the UI, to ensure all current notices are available to the consumer.
 - In addition, EDE partners must take over the Application Submission and DMI Creation Communications.
 - Note that the method, wording, and format of how the partner communicates this to the consumer do not need to mirror CMS’s current method (i.e. does not need to be two separate e-mails as CMS executes currently), so long as the EDE partner is reasonably communicating the contents to the consumer. (i.e. the goal is for the consumer to be educated/alerted about the above in a way that they will understand the information.)
 - Partners may improve these communications in contrast to CMS’s default, based on their knowledge of the consumer (examples: Combine the Application Submission & DMI creation information into a single message about next steps & action items; leverage the User Interface to reinforce key items to the consumer, etc.)
 - For additional information regarding the communication requirements for EDE, please review the communications toolkit on CMSzONE: <https://zone.cms.gov/document/enhanced-direct-enrollment-edc-documents-and-materials>
 - Note also, CMS is currently looking into the possibility of providing partners with push notifications when new notices become available, and if that functionality is able to be implemented at some point in the future, partners would then become responsible for notifying consumers when new notices become available.
- 2. The Communications toolkit says that DE Entities must notify consumers with action items that the consumer must take. It says they must be communicated in the consumer's account, and through email and text. Is text a requirement? Is there additional information beyond the two required notifications (Application Submission and DMI Creation Communications) that we must provide?**

- In addition to providing the Application Submission and DMI Creation Communications, DE Entities must provide and communicate ongoing statuses and access to information for consumers to manage their application and coverage. These communications include, but are not limited to, statuses of DMIs and SVIs, special enrollment periods, providing and communicating about new notices generated by the FFE, application and enrollment status, and supporting document upload for DMIs and SVIs.
- There is no exhaustive list of the type of information that needs to be communicated to consumers. The information communicated would be similar to the type of information that CMS currently communicates to consumers via the consumer's MyAccount page at HealthCare.gov. DE Entities can also review the API documentation on CMSzONE.
- Partners can choose whether to offer text as a communication option to the consumer in the UI (i.e., it is optional).

4.0 Upstream Entity FAQs

1. What information and/or documents are upstream entities required to submit to CMS for participation in EDE?

- Most of the audit will be handled by the primary entity if the upstream entity is not changing anything on the EDE platform aside from branding. Please review the EDE Onboarding checklist located on the CMSzONE EDE Documents and Materials page at the following link for a list of the information and documents that the primary and/or upstream entity are required to submit (CMS will make periodic updates to this checklist):
<https://zone.cms.gov/document/enhanced-direct-enrollment-edc-documents-and-materials>.

2. The EDE Auditor Guidelines published on February 21, 2018 state the following: “The upstream entity will be responsible for complying with all requirements in regulation, applicable guidance, and the EDE Agreement, including oversight of the entity providing the EDE pathway.” How should the upstream entity oversee the primary entity?

- The upstream entity will not be approved to use EDE until the primary entity meets all requirements.
- The upstream entity is responsible for reviewing and attesting that the ORR audit submitted on its behalf accurately represents its pathway's compliance (details to follow).
- Per 45 C.F.R. § 156.340(b), as part of any downstream agreement with any vendor, anything the vendor is agreeing to do should be listed out in the Agreement between the upstream and primary entity.

3. What are the requirements for EDE API transactions originating from upstream entities?

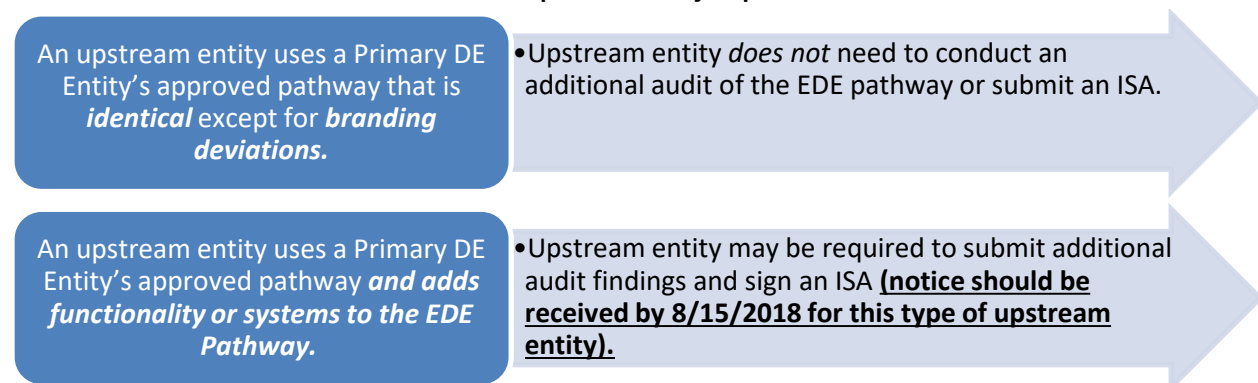
- CMS will be requiring EDE Partners with upstream entities to submit EDE API transactions using Partner IDs of the upstream entities, when EDE applications/enrollments originate from the upstream entities.
 - For example, Issuer A is an upstream entity that uses your platform, but consumers remain on Issuer A's customized site/URL for enrollment
- CMS will not require a Partner ID for an A/B that uses a primary entity's platform by redirecting consumers to the primary entity's site/URL for enrollment
- CMS will require primary entities to send Partner IDs of upstream entities when a EDE Business Agreement is required of the upstream entity
 - CMS is requiring this for a variety of reasons: For reporting/tracking purposes, CMS wants the application/policy documents to reflect the entity that the transaction originated from
 - For privacy reasons, only the entity from which the transaction originated from should have access to the consumer's records via the EDE APIs Reminder: When permission is stored via the EDE Permission API, access will be restricted for most of the EDE APIs based on the Partner ID that is used during the transaction Access is not restricted based on permission for the following APIs: Person Search, RIDP/FARS, Store ID Proofing, Create App, Reference Data
 - For purposes of suspension, CMS will be able to suspend specific Partner IDs If only one Partner ID is used by the primary entity, a suspension of either the primary entity or any single upstream entity would result in the suspension of all activity from any entity using that Partner ID.
- A DE entity who has upstream entities must notify CCIIO of the name, Partner ID, and primary point of contact (POC) of each upstream entity that will use its EDE pathway.
- Each upstream entity must have a unique Partner ID.
 - Each upstream entity will receive a Partner ID when the Primary DE Entity submits the Onboarding Form to the Hub.
 - The Primary DE Entity must complete the updated Hub Onboarding Form, to include additional information for each of their upstream entities. The form will be emailed to dsh.support@qssinc.com.

4. **Can CMS provide clarification on what defines an upstream entity? For example, if a web-broker decides to white label its site and have different agent/brokers use its portal and give them the ability to change some landing page graphics, would they be considered upstream entities? If there are different portals that are issuer specific, would each have to be declared as an upstream entity?**
- A web-broker or issuer may choose to develop its own EDE pathway or use a CMS-approved EDE pathway provided by another entity (a “provider” or “primary entity”). If a web-broker or issuer uses the EDE pathway of a provider, the web-broker or issuer will be an “upstream entity” of its provider. Any upstream entities are subject to specific requirements regarding their use of the provider’s EDE pathway included in the EDE Business Agreement (updated June 20, 2018) and available here: <https://zone.cms.gov/document/enhanced-direct-enrollment-edo-documents-and-materials>. In particular, please review Section VI “Use of DE Entity’s EDE Pathway by Downstream and Delegated Entities” and Section VII.e “Use of an EDE Pathway Provided by Another Entity.”
 - Additionally, CMS posted a slide deck from the April 25, 2018 EDE Upstream Entity Webinar. The deck provides information about upstream entity scenarios, requirements, oversight, upstream entity Partner ID requirements, and resources for upstream entities. The deck is available on CMSzONE here: https://zone.cms.gov/system/files/documents/ede_upstream_entity_webinar_slides_final_4-25-18.pdf.

Upstream Entity Expectations

- CMS encourages DE Entities to submit upstream entity information as soon as possible (including the URL to the upstream entity's EDE website).
- However, DE Entities should submit any upstream issuers no later than 10/15/2018 and any upstream web-brokers no later than 10/1/2018.

Exhibit 6. Upstream Entity Expectations



10/09/18 Update

- CMS previously messaged that issuers have until October 15 to partner with a primary entity who intends to provide an EDE pathway during the 2019 OEP.
- **DE Entities may submit upstream entities to CMS up until they go live with EDE;** CMS will review and approve pending resources at the time received.
 - Note: Partner go-live dates will largely depend on the quality and completeness of the audit submission; as previously stated, CMS does not guarantee go-live dates.
- Primary entities must email directenrollment@cms.hhs.gov to confirm any upstream issuers who will use their EDE pathway. CMS will require written confirmation from upstream entities as well, as well as required information and documentation from the upstream entities as requested.

5.0 General

These FAQs cover compliance topics applicable to all DE Entities and auditors.

1. Can an auditor perform both the business and privacy/security audits?

- Yes. Per Section IV, “Selection of Auditor,” in the [EDE Auditor Guidelines](#), the DE Entity is permitted to select either one auditor to complete both the business requirements audit and the privacy and security audit, or the DE Entity may select two auditors: one to complete the business requirements audit and another to complete the privacy and security audit.
- Auditors are permitted to subcontract these activities; however, a DE Entity must disclose any subcontracting arrangements by its auditors in the DE Entity’s EDE Agreement and/or ISA with CMS and disclose any potential conflicts of interest consistent with the EDE Agreement.

2. Is there a deadline for adding upstream entities?

- To allow enough time for upstream entities to complete applicable requirements, DE Entities should notify CMS of upstream entities using their pathway as soon as is feasible. CMS encourages DE Entities to notify CMS no later than August 15, 2018. *Update: DE Entities should submit any upstream issuers no later than 10/15/2018 and any upstream web-brokers no later than 10/1/2018.*

3. What is the purpose of CMS’ secure documentation upload portal? When should I use it? How does my organization get access to the secure documentation upload portal? Do I receive a confirmation when I upload a document to the secure portal?

- The purpose of the portal is to provide a secure method for DE Entities to submit proprietary information to CMS.

- Primary points of contact (POCs) for DE Entities that are developing a pathway received instructions the week of February 19 on accessing the secure portal and submitting documentation using their unique access code. Upon request, the DE Help Desk (directenrollment@cms.hhs.gov) can email these instructions and access code again. CMS will also be providing access to the secure portal to upstream entities that sent a notice of intent who confirmed a primary POC within their organization.
 - DE Entities and their upstream entities must submit the following documents via the secure portal, as applicable: Privacy questionnaire, application UI feedback requests, EDE Agreement, ISA, business audit, and privacy and security audit documentation. This list may not be exhaustive, and DE Entities are encouraged to upload any other documents that may contain sensitive material through the portal. The DE Entity will receive confirmation when the secure portal has successfully uploaded the files to CMS.
- 4. Will a primary entity have its own Partner ID? Which Partner ID should be used for the APIs?**
- If you are a Third-Party Administrator and you only provide your pathway to upstream issuers, and are not enrolling any consumers outside of the issuer's pathway, you would not have your own Partner ID.
 - If you are a web-broker, you need a Partner ID for your line of business and a Partner ID for each upstream entity.
 - If the enrollment is on behalf of an issuer, the primary entity must use that issuer's Partner ID in the API request.
- 5. Will CMS provide a list of primary DE Entities that are building EDE pathways?**
- CMS will provide a list of DE Entities (primary and upstream issuers and web-brokers) approved to use EDE. That list will include phases that the DE Entity is approved for.
 - The list of entities (both primary and upstream) that were approved to use proxy DE for 2018 OE is available on the CCIIO website here: <https://www.cms.gov/CCIIO/Programs-and-Initiatives/Health-Insurance-Marketplaces/Downloads/DE-Proxy-Partner-Public-List.pdf>
- 6. Will EDE work for dental plans or is it only for medical plans? Can dental carriers only display their own dental plans through the EDE interface? Is it permissible for an upstream entity to offer all medical plans, but only its own dental plans?**
- A consumer cannot enroll in dental-only plans through DE. EDE will operate similar to Classic DE today, in terms of enrollment submission. At this time, CMS does not allow dental-only enrollment submissions via DE/EDE. CMS does allow dental enrollment via DE/EDE, but the dental enrollment must be in conjunction with a health plan enrollment.

- An upstream issuer must offer its own QHPs if they will also offer dental plans via DE/EDE. In that scenario, the issuer is permitted to limit the display to its own QHPs and dental plans via DE/EDE. Further information about website and QHP display requirements for web-brokers and issuers using DE can be found in the latest Federally-facilitated Marketplace (FFM) and Federally-facilitated Small Business Health Options Program (FF-SHOP) Enrollment Manual: <https://www.cms.gov/CCIIO/Programs-and-Initiatives/Health-Insurance-Marketplaces/General-Resources-Items/FFM-and-FF-SHOP-Enrollment-Manual.html?DLPage=1&DLEntries=10&DLFilter=enrollment%20manual&DLSort=0&DLSortDir=descending>.
- 7. **The 2019 Notice of Benefit and Payment Parameters (NBPP) rule finalized a revision to section 45 C.F.R. § 155.221 indicating issuers are now subject to the auditor requirement for DE. Does this requirement now apply to classic DE (double redirect) Partners, EDE Partners, or both? If it applies to EDE Partners, how is this different than the current auditor process for EDE Partners?**
 - The third-party auditor requirements for DE outlined in 45 C.F.R. § 155.221 apply only to those issuers participating in EDE (i.e., planning to host the platform or create the technology solution to connect to the APIs and HUB). Issuers utilizing classic DE are not subject to that requirement and do not need to hire an auditor to review that flow. The audit cited in 45 C.F.R. § 155.221 relates to the current auditor process for DE Entities using the EDE pathway and should reference the guidance found at <https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Third-party-Direct-Requirements.pdf> for clarification.
 - Additionally, issuers that want to only gain access to the Marketplace consumer records (MCR) API (which is one of the APIs used for EDE), are subject to the same privacy/security audit and agreement as the DE Entities using EDE, but these issuers are exempt from signing and submitting the EDE business agreement. Please note that this is an optional service that issuers can utilize to help them with casework/get real time enrollment updates but is not required. Issuers should determine if the requirements to gain access to that service will be worth the value of using that service.
- 8. **Do primary and upstream entities need to provide National Producer Numbers (NPNs) to CMS?**
 - No, primary and upstream entities will need to provide Partner IDs instead of NPNs (only applicable for DE Entities operating as web-brokers).
 - CMS is updating a previously shared data request so that DE Entities are aware that NPNs will not be needed.

9. What are the requirements for a DE Entity using EDE to be listed on HealthCare.gov with a link (URL) to its website?

As a resource for consumers, CMS will provide a list of URLs from approved DE Entities (QHP issuers and web-brokers) using EDE that will allow consumers to access these entities' websites directly from HealthCare.gov. CMS is currently working on the technical development for the display of URLs and will provide additional details as they become available.

All DE Entities using EDE will need to submit the URL they would like CMS to use for this purpose. To have their URL displayed, in addition to meeting current CMS regulations and guidance regarding QHP display,⁶ DE Entities will need to meet the following requirements:

- **URL Requirements:** The website URL must take consumers directly to the beginning of the QHP shopping experience on the DE Entity's website. CMS considers the QHP shopping experience to begin with a DE Entity collecting information specifically to display QHP options to consumers or to populate Exchange eligibility applications. The URL should not direct consumers to a general landing or homepage where consumers have to take another action to indicate they wish to shop for QHPs.
- **Branding Requirements:** Within the QHP shopping experience, a DE Entity must use language consistent with the Marketplace program when referencing the program, types of coverage, benefits, and processes on its website (e.g., "Marketplace coverage," "Health Insurance Marketplace").
- **Ancillary Products Marketing Requirements:** DE Entities must comply with current CMS guidance regarding ancillary products marketing. Please reference the *FAQ Regarding Ancillary Products Marketing for Direct Enrollment (DE) Entities* that CMS released in June 2018, available on the Issuer and Web-broker Community pages on CMSzONE.⁷

CMS will be conducting website reviews of DE Entities' websites for compliance with these requirements. If CMS finds that a DE Entity does not meet one or more of the above requirements, the entity's website URL may not be displayed.

⁶ **Web-brokers:** 45 C.F.R. §§ 155.220(c)(3) and (j)(2), *Guidance for Web-brokers Registered with the Federally-Facilitated Marketplaces* (October 2016): <https://www.cms.gov/CCIIO/Programs-and-Initiatives/Health-Insurance-Marketplaces/Downloads/Guidance-Web-brokers-FFMs.pdf>, and *Guidance for Web-brokers on Displaying Mandatory Standardized Disclaimers* (April 2015): <https://www.cms.gov/CCIIO/Programs-and-Initiatives/Health-Insurance-Marketplaces/Downloads/Guidance-Web-brokers-Displaying-Disclaimers.pdf>; **QHP Issuers:** 45 C.F.R. § 156.1230; **Both:** *Federally-Facilitated Exchange (FFE) and Federally-Facilitated Small Business Health Options Program (FF-SHOP) Enrollment Manual* (June 2018): <https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Enrollment-Manual-062618.pdf>.

⁷ Web-broker Community: <https://zone.cms.gov/document/web-broker-guidance-and-frequently-asked-question-faq-documents>; Issuer Community: <https://zone.cms.gov/document/direct-enrollment-de-documents-and-materials>

10. What is the CMS-Initiated Change Request Process for DE Entities Using EDE in Plan Year 2019?

This FAQ outlines the process DE Entities must follow when CMS releases EDE-related changes that must be implemented by DE Entities using or pursuing EDE. The process for DE Entities that wish to initiate changes of their own will be outlined in a different FAQ.

CMS may require DE Entities to implement new or updated EDE requirements, including updates to business requirements audit toolkit versions that are released after the date of the CMS-designated baseline version of each toolkit (within this document see “Does CMS have any guidance for using the updated Business Requirements Audit Report Template and toolkits once we have begun the business requirements audit?” for more information about the baseline toolkit versions). These required revisions will be considered CMS-initiated change requests (CRs).

DE Entities have two options to implement required revisions:

- Submit supplemental documentation; or
- Have their Auditor review the required revision as part of the business requirements audit. For example, if the required revision is in a toolkit, the Auditor will use the version of the toolkit containing the revision(s) to complete the business requirements audit.
 - *Note: Auditors do not have access to the EDE Change Request Tracker (see below). DE Entities must provide a copy of the Change Request Tracker to their Auditor(s).*

All DE Entities participating in EDE must implement CMS-initiated CRs. However, depending on when a DE Entity submits its business requirements audit in relation to when CMS notifies DE Entities about a required CR, the CR may be audited as part of the business requirements audit or the DE Entity may demonstrate that it has implemented the CR as part of a separate process. Specifically:

- DE Entities that have already submitted their business requirements audit *before the CR is released* must submit evidence of their implementation of the CR in clearly labeled supplemental documentation, rather than have their Auditor re-review the portion of the audit affected by the CR.
- DE Entities that submit their audits *after the CR is released, but before the implementation deadline* have two options: (1) they may have their Auditor review the CR as part of the business requirements audit or (2) they may provide clearly labeled supplemental documentation of their implementation of the CR anytime up until the implementation deadline stated in the EDE Change Request Tracker (explained below).
- DE Entities that submit their audits *after the CR implementation deadline* will be required to submit documentation of their implementation of the CR with their audit submission (either incorporated in the Auditor's review or in clearly labeled supplemental documentation).

CMS Change Request Tracker

CMS will specify the changes that DE Entities are *required* to implement via the EDE Change Request Tracker, which is posted on the EDE Documents and Materials page on CMSzONE, located here: <https://zone.cms.gov/document/enhanced-direct-enrollment-edo-documentsand-materials>.⁸

The EDE Change Request Tracker is a spreadsheet containing information about each CMS-initiated CR, including a description of each CR; the EDE document in which the CR appears; whether the DE Entity must submit documentation to demonstrate compliance and, if so, the type of documentation the DE Entity must submit (e.g., if DE Entities must submit screenshots or notify the DE Help Desk when the change is implemented); the deadline for submission of documentation; the method of submission of required documentation; and conditional requirements, if applicable. The Change Request Tracker only describes the CR; the DE Entity must review the CR within the identified EDE document.

Deadlines for Implementation of Required Changes and Potential Penalties

CMS will attempt to provide as much notice to DE Entities as feasible regarding CMS-initiated CRs. Per the EDE Business Agreement, CMS will provide a timeline for each CMS-initiated CR for DE Entities to implement the change.

While CMS anticipates that this will be a rare occasion, some CMS-initiated CRs may require significant revisions to the EDE pathway that would require independent verification by a Third-party Auditor. CMS will provide advance notice to DE Entities in the event CMS requires a CMS-initiated CR of this type. If DE Entities don't timely submit documentation of their implementation of such CRs, CMS may suspend the non-compliant DE Entity's EDE pathway.

If a DE Entity does not meet the deadline to show implementation of the CR and has not already gone live with EDE, the DE Entity will not be able to go live until submitting the appropriate documentation.

Implementation of Optional Changes

Changes that appear in an EDE document that are *not* included in the Change Request Tracker are considered optional to implement.

- If a DE Entity wishes to implement an optional requirement and *it has already submitted its business requirements audit*, it must notify CMS and submit (via the secure portal) clearly labeled documentation that confirms the implementation of the optional requirement.
- If a DE Entity wishes to implement an optional requirement and *it has not already submitted its audit*, it may have its Auditor review the optional requirement as part of the business

⁸ CMS restricts CMSzONE access to web-brokers and issuers only.

requirements audit. For example, if the optional requirement is in a toolkit, the Auditor will use the version of the toolkit containing the revision(s) to complete the business requirements audit or include clearly labeled supplemental documentation of implementation as part of its audit submission.

11. How should the Auditor document issues it encounters during the audit?

- Auditors may come across technical testing issues during the business audit that prevent the Auditor from completing the review of specific requirements in the toolkits.
- When this happens, CMS encourages Auditors to troubleshoot the issue with the DE Entity and CMS before submitting the audit.
- Auditors should make sure to document any access or other issues—resolved or that could not be resolved—within the toolkits and templates under risks, mitigation strategies, etc.
 - Any related conversations between the partner and CMS should be referenced within the submission.

12. Reminders about the EDE Business Agreement

- Please make sure to submit the updated EDE Business Agreement (dated 6/20/18) that is available on zONE.
- **Appendix H: End-state Phase Selection:** Upstream entities should coordinate with the entity providing the pathway to complete the phase that the primary entity will implement.
 - If implementing an identical pathway, it is not possible for an upstream entity to implement a different end-state phase than the primary entity providing the pathway.
- All primary and upstream entities must submit a complete Agreement and fill out all fields within the body of the Agreement and appendices.

13. What Types of Changes May a DE Entity Make to a CMS-approved EDE Pathway, and What is the Process to Notify CMS?

The following FAQs and answers provide additional detail and clarification regarding the process that DE Entities hosting an EDE pathway must follow prior to making any changes to an EDE pathway that was audited by a third-party auditor and approved by CMS for use in plan year 2019. This process is specific to DE Entity-initiated changes (i.e., not CMS-initiated changes). The process to implement CMS-initiated change requests (i.e. changes to toolkits and the business requirements audit report template that CMS requires DE Entities to implement) and

optional changes to toolkits and the template is provided in a different FAQ.⁹ The DE Entity must continue to comply with requirements of the configuration management control family as outlined in the Non-Exchange Entities (NEE) Security and Privacy Plan (SSP) workbook.¹⁰ All changes must be tested, validated, and documented before implementing the changes in the operational system.

Change Categories

In the table, CMS is providing a categorization of the types of changes a DE Entity might make to their EDE pathway with examples. The process for implementing a change within each category is provided below the table. DE Entities are not required to notify CMS of any changes made to their EDE pathway that do not fall under the scope of one of the below change categories. The table is intended to serve as a guideline for DE Entities; DE Entities should contact the DE Help Desk (directenrollment@cms.hhs.gov) if they are unsure what category a change falls under.

Exhibit 7. Change Categories for Partner-Initiated Changes

Brief Description	Examples of Changes in this Category	Change Category
These changes include any system or software updates that do not alter the privacy and security status of the EDE pathway as represented in the CMS-approved audit or changes to the EDE pathway that have no effect on the consumer's user interface (UI) experience. Can include significant changes in entities' communication strategy	• System version updates • Fixes to typos and other bugs • Changes to design elements such as color, font, navigational menus, etc. • Changes to DE Entity branding or DE Entity support channel contact information • Addition of CMS-approved help text language provided in the Application UI Toolkit, Phase 1 Screening Questions, Phase 2 Screening Questions, and Phase 3 Screening Questions tabs under the column entitled "Question Help" and the UI Questions tab under the column entitled "Informational Text"	Category 1: Changes that require CMS notification, but that CMS does not need to approve

⁹ See "What is the CMS-Initiated Change Request process for DE Entities using EDE in Plan Year 2019?" within the EDE Compliance FAQs.

¹⁰ The NEE SSP workbook is available on the EDE page on CMSzONE: <https://zone.cms.gov/document/enhanced-direct-enrollment-edo-documents-and-materials>

Brief Description	Examples of Changes in this Category	Change Category
with consumers that don't impact the UI. These changes may also include modifications to the information presented to consumers, applicants, qualified individuals, or enrollees regarding eligibility, the eligibility application, the eligibility determination, and enrollment processes if CMS has previously messaged that it is a permissible change.	Significant changes in how the entity communicates with consumers on required actions and about new status information (i.e. communications about notices, data matching issue [DMI] deadlines, etc.) where a significant change in messaging (that CMS has messaged is permissible), frequency, or method is made. For example, changing email communications on DMI deadline reminders from once a week to daily, or stopping communications (emails, texts, calls) on something the consumer still needs to do.	
These changes include any modifications to the information presented to consumers, applicants, qualified individuals, or enrollees regarding eligibility, the eligibility application, the eligibility determination, enrollment processes, status, action items, and related communications about eligibility and enrollment. These changes do <u>not</u> include modifications to the information presented to consumers, applicants, qualified individuals, or enrollees regarding eligibility, the eligibility application, the eligibility determination, and enrollment processes if	• Minor changes to the consumer's UI, including the application or enrollment experience, that go beyond the changes described above. For example, changes to the wording of a set of questions and answers not explicitly described in the UI Question Companion Guide, or changes to whether previously entered information is pre-populated when the applicant reports a life change. • Changes to the eligibility application that add or remove questions from displaying for any eligibility scenario - o For example, adding a question or tool to help consumers calculate their projected annual income • Changes to the eligibility application that change the order of questions, or the conditional logic for when questions appear - o For example, making a change to ask the Medicaid block questions	Category 2: Changes that require CMS notification and pre-approval, with accompanying documentation

Brief Description	Examples of Changes in this Category	Change Category
CMS has previously messaged that it is a permissible change (this falls within Change Category #1, as set forth above).	after the income questions instead of before • Changes to account management capabilities (application and enrollment statuses, notices, consumer action items, etc.). ◦ For example, changes to the wording of a set of questions and answers or changes to how DMI and special enrollment period verification issue (SVI) status and notices are displayed and communicated to consumers	
These changes include any modifications to the systems comprising the EDE pathway to the extent that the CMS-approved audits and existing Interconnection Security Agreement (ISA) no longer accurately reflect the compliance of the pathway.	• Adding new systems to the EDE pathway, adding or removal of upstream entities that interact with consumer data provided by the Exchange • Significant code changes¹¹ • Moving to a new data center • Altering the way consumers access the application (e.g., moving it from an internal system to an external system) • Changes to the scenarios supported by the eligibility application or transition to a different eligibility application phase.	Category 3: Changes that require CMS notification, pre-approval, and verification by an independent third-party auditor

Process for Implementation of Changes within Each Category

- **Change Category 1 - Changes that require CMS notification, but that CMS does not need to approve:** DE Entities must email the DE Help Desk (directenrollment@cms.hhs.gov) and detail the scope of the change. The email subject line

¹¹ Per National Institute of Standards and Technology (NIST) SP800-37, significant changes to an information system may include, for example: (i) installation of a new or upgraded operating system, middleware component, or application; (ii) modifications to system ports, protocols, or services; (iii) installation of a new or upgraded hardware platform; (iv) modifications to cryptographic modules or services; or (v) modifications to security controls. Examples of significant changes to the environment of operation may include for example: (i) moving to a new facility; (ii) adding new core missions or business functions; (iii) acquiring specific and credible threat information that the organization is being targeted by a threat source; or (iv) establishing new/modified laws, directives, policies, or regulations.

must start with “Category 1 Change.” DE Entities may submit accompanying documentation, but it is not required. DE Entities should submit any accompanying documentation through the secure portal.

- **Change Category 2 - Changes that require CMS notification and pre-approval, with accompanying documentation:**
 - DE Entities must email the DE Help Desk (directenrollment@cms.hhs.gov) and detail the scope of the change that they intend to make. The email subject line must start with “Category 2 Change.” DE Entities must submit accompanying documentation through the secure portal. Examples of documentation include a mock-up of the UI or a screenshot from within the DE Entity’s testing environment that demonstrates the intended change.
 - This type of change requires pre-approval from CMS; CMS will review the change and respond to the DE Entity. CMS cannot guarantee a response timeframe but will respond as soon as resources permit. CMS will either confirm that the DE Entity can proceed or may request additional information.
- **Change Category 3 - Changes that require CMS notification, pre-approval, and verification by an independent third-party auditor:**
 - DE Entities must email the DE Help Desk (directenrollment@cms.hhs.gov) and detail the scope of the change that they intend to make, how the auditor will review the change, and what documentation the auditor will prepare. The email subject line must start with “Category 3 Change.” Examples of documentation prepared by the auditor include an updated Plan of Action and Milestones (POA&M), updated toolkit, or an updated Security and Privacy Assessment Report (SAR). At this step, DE Entities may submit accompanying documentation through the secure portal if it would be helpful for CMS review.
 - The DE Entity must email the request to CMS for pre-approval prior to implementing the change and having it verified by a third-party auditor. CMS will review the change and respond to the DE Entity. CMS cannot guarantee a response timeframe but will respond as soon as resources permit. CMS will either confirm that the DE Entity can proceed or may request additional information.
 - After the auditor verifies the change, the DE Entity must submit the documentation prepared by the auditor (previously approved by CMS).

Please contact the DE Help Desk with any questions.

14. Are there any restrictions for DE and EDE Entities (issuers; web-brokers; agents and brokers; primary EDE Entities; upstream EDE Entities; and hybrid, non-issuer

upstream EDE Entities) accessing the FFEs with an IP address that is outside of the United States of America (USA)?

Any EDE Entity or web-broker and its assignees or subcontractors—including, employees, developers, agents, representatives, or contractors—cannot remotely connect or transmit data to the FFE or its testing environments, nor remotely connect or transmit data to an EDE Entity’s or web-broker’s systems that maintain connections to the FFE or its testing environments, from locations outside of the United States of America or its territories, embassies, or military installations. This includes any such connection through virtual private networks (VPNs).

5.1 Training

1. Which training modules are auditors required to complete prior to initiating the privacy and security audit and business audit for EDE?

- An auditor who will just be completing the privacy and security audit:
 - Must complete the EDE Regulatory/Compliance Standards module;
 - Must complete the EDE Privacy/Security Standards module; and
 - Is no longer required to complete the EDE ORR and CMS Reporting Requirements module as that training will only review business audit templates and reporting.
- An auditor who is only completing a business audit must complete the following training modules prior to initiating the business audit:
 - EDE Regulatory/Compliance Standards,
 - EDE Application UI Overview, and
 - EDE UI Services.
 - EDE ORR and CMS Reporting Requirements (note: Although it is **no longer required that DE Entities and auditors complete this module prior to conducting the business audit**, they must complete the module before ***submitting*** the business audit. The module provides DE Entities and auditors with an overview of the Business Report template and toolkits.)
- Representatives from primary DE Entities must take all training modules; CMS encourages representatives from upstream entities to take all trainings as well.

2. Are there specific guidelines on who must take training modules and whether different members of the audit team can take different training modules? Is the same auditor representative required to take all trainings?

- It does not need to be one person completing all training modules from the auditor or DE Entity organization. The person that will do the audit must complete each relevant training. Partners should notify CMS of auditors who are completing the required trainings.

Appendix A. Sample Security Design (Adapted by CMS)

A PDF of Exhibit 8 is also available as a zip file on the EDE zONE page under FAQs.

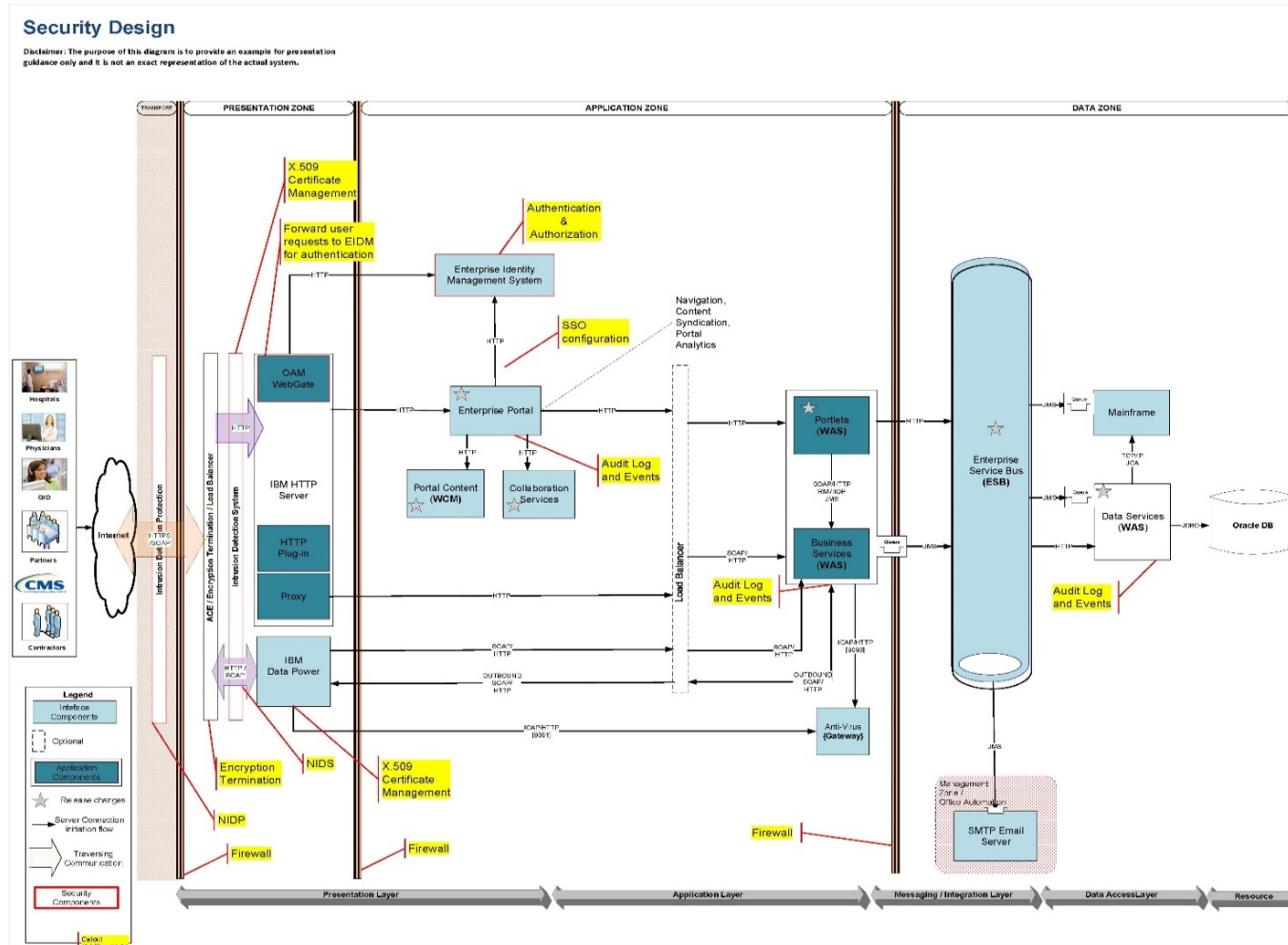


Exhibit 8. Sample Security Design (Adapted by CMS) (Full-size)

Appendix B. 7 Tips for Building an API-Secure Architecture



7 tips for building an API-secure architecture¹²

By Darryn Graham

May 17, 2018

Application programming interfaces are a common tool for powering public sector engagement, but when APIs are under protected, agencies leave themselves vulnerable to attack. The risk is so acute that the Open Web Application Security Project added Under protected APIs to its OWASP Top 10 security risks of 2017.

Because APIs expose systems of record that typically reside within an agency's trusted network, additional considerations must be made to avoid security risks that exposure can create. Organizations can mitigate many of the risks by using an API gateway to facilitate these requests.

API gateways act as a specialized proxy server that controls the requested traffic, detects and defends against distributed denial-of-service attacks and leverages existing investments in malware/antivirus scanners. Below are seven key best practices to consider when designing a secure architecture needed to implement a trusted API gateway:

1. Control requests into the agency's trusted network. The API gateway should not permit connections directly into the ATN that originate from the network's demilitarized zone. Instead, an internal gateway component in the ATN should connect outward to the API gateway in a tunneled fashion. This approach removes the need to open incoming firewall ports from the DMZ into the ATN, preventing any connections from servers in the DMZ should they become compromised. Additionally, connections from the ATN to the API gateway should be persistent, so that encryption handshakes are not continually re-established, which can negatively impact performance.
2. Establish filtering rules and alerts. The API gateway should be configurable to actively filter requests based on agency security and operating policies. Filters should include the ability to block specific IP address ranges and to act dynamically based on request type, endpoint name, request payload size and authentication. Automated alerts should be sent to system administrators and management dashboards when requests violate filter rules.

¹² Source: Graham, D. (2018, May 17) "7 tips for building an API-secure architecture." Retrieved from <https://gcn.com/articles/2018/05/17/api-gateway.aspx>

3. Implement protective caching. Depending on the data and use case, the API gateway should be employed to store and serve frequently accessed data directly from caches of random-access memory. This provides a high-performance buffering layer that can insulate the internal endpoint from spikes in volume. In addition to protecting the internal endpoint, this technique increases API service performance, facilitates scalability and decreases internal network traffic. For example, a weather API might only deliver updated data every five minutes, but during a hurricane the API might be inundated with concurrent requests. In this use case, protective caching could provide an extremely affordable scaling mechanism that helps the data provider avoid sizing its architecture to accommodate unpredictable spikes in utilization.

4. Operationalize cyber threat information. The API gateway itself should provide flexible administrative APIs to allow for fast, automated and scripted configuration. With a dynamically configurable API gateway, agencies can quickly operationalize actionable threat indicators from the National Cybersecurity and Communications Integration Center. Additionally, certain rule violations or alerts triggered on an agency's API gateway may reveal threats that should be shared with the cyber community through the Department of Homeland Security's Automated Indicator Sharing service.

5. Manage identity and access. The API gateway should provide a robust policy action to effectively identify and validate clients, with the ability to support a wide variety of identification and authorization options. This gives agencies flexibility to identify clients who are trying to access the APIs. At a minimum, the gateway's supported identification options should include: hostname address, API key, IP address change, SSL certificate, OAuth2 token, XPath expression, WSS username token and WSS X.509 certificate.

6. Protect against payload threats. Another important factor is how the API gateway blocks attacks coming through JSON or XML string lengths and payloads by setting:

- Maximum number of entries allowed in an object.
- Maximum string length allowed for a property name within an object.
- Maximum number of elements allowed in an array. It should also specify XML attributes such as:
 - Maximum number of characters permitted in the namespace prefix.
 - Character limit for any namespace universal resource identifiers present in the XML document.
 - Maximum number of child elements allowed for any element.
 - Maximum node depth allowed in the XML.

7. Deploy SQL injection filters. The API gateway should include the ability to block SQL query requests based on custom blacklisted items, such as invalid special characters. The ability to dynamically configure rules gives agencies maximum flexibility to adjust as new threats are identified.



Employing an API gateway and following these steps is a proactive way for agencies to address specific security challenges to data and applications that require open, public access. Although no security solution is ever complete, agencies must deploy the latest security techniques to reduce their risk profile. An API that fails to deliver the expected level of security, reliability and performance can have tremendous mission impacts -- to both the organization producing it and those consuming it.

About the Author:

Darryn Graham is chief architect at Software AG Government Solutions.