Report to the Mozilla Community

June 7, 2024

Contents

1. Executive Summary

Entrust has prepared this response to Ben Wilson's May 7, 2024 letter to the Mozilla community**.** We see this as an opportunity to improve how we serve the ecosystem and our subscribers as a Certificate Authority, and to provide learnings, insights, and actions that will benefit the web ecosystem.

We will review recent key incidents and their root causes across four areas, and provide a detailed overview of concrete, measurable steps we are undertaking to address root causes and improve operations:

- **Incidents Related to Ballot SC-62v2** – This section addresses what happened and how we will prevent future incidents.
- **Incident Handling & Communication** – This section addresses instances where we have not met requirements and expectations, and how we will improve.
- **Documentation Updates** – This section reviews incidents around policy updates, and how we will enhance our processes.
- **Delayed Revocation** – This section discusses recent incidents and commitments around delayed revocation, and how we are advancing our position, resources, and capabilities to meet the requirements.

Entrust has been a certification authority for over two decades, and we have strived to be a positive influence on development and advancement of our industry's standards since the CA/Browser Forum was created in 2005. We recognize that these incidents were unnecessary and based on our own mistakes or misjudgments – in this we fell short of the high standard we set for ourselves. We have thoughtfully considered the community's questions and comments, and this input is reflected in our plans.

We also want to make clear that we believe there should be no conflict between meeting the baseline requirements and minimizing disruption. Subscribers – and the whole web ecosystem – are more secure and resilient when we support them with the people, processes, and tools that enable 24-hour or five-day revocation should the need arise.

The recent incidents have root causes that must be addressed. Entrust is focused on making substantive improvements, and you will find in-depth plans and timelines in this report.

Highlights include:

People

- **Organization:** Adding strategic support for compliance with CA/Browser Forum and root program requirements by aligning our CA team with Entrust corporate compliance and IT operations and making additional investments in people and tooling.

- **CA/Browser Forum:** Planning to broaden the team required to execute CA/Browser Forum requirements and expectations, and to broaden Entrust participation to include product experts and leaders.

Process

- **Compliance Governance:** Enhancing internal governance with a cross-functional change control board to review policies and key decisions to ensure they comply with requirements.
- **Change control:** Improving and filling gaps in our change control process to minimize errors. Tightening processes, including change management and CCADB monitoring.
- **Policy Improvements:** Reviewing and clarifying incident response and revocation policies to align with requirements. Improving policy to update processes and controls when updating our documentation (e.g. CPS).

Technology

- **Expand Pre- and Post-Linting**
  - Assign product manager responsible for linting.
  - Reserve capacity in every product release cycle for linting updates and improvements.
  - Contribute new lints and identified improvements back to open-source community.
- **Automation**
  - Improve Certificate Lifecycle Management (CLM) automation capabilities for our subscribers.

As of June 7, 2024, all affected certificates related to these incidents have expired or been revoked.

This report, and the extensive plans behind it, are the result of a cross-functional effort. Members of our product, compliance, development, legal, operations, support, and executive leadership teams contributed to the preparation of this report. We also retained a third-party consultant, industry expert Don Sheehy, to assess pertinent Entrust processes and make recommendations for improvement. We want to thank him for his contributions.

2. Review of Issues and Root Causes

In each of the following sections, we will describe the issues, analyze root causes, and lay out an improvement plan to address these issues. Appendix 1 contains the full bug list. Appendix 2 contains a consolidated list and timeline for planned improvements.

2.1 Incidents Related to Ballot SC-62v2

2.1.1 Issue Description

On September 11, 2023, Entrust made updates to its TLS certificates that were intended to meet the updates to the TLS Baseline Requirements mandated by the CA/Browser Forum's Ballot SC-62v2. Recent incidents detailed below stemmed from how we implemented these updates.

EV Certificates missing cPSuri (#1883843): We interpreted the guidance to 'not include' the cPSuri in OV TLS certificates – a change intended to reduce the file size of certificates – to also

apply to EV certificates. However, the requirement to include the cPSuri remained in the EV Guidelines. Entrust removed the cPSuri from EV certificates in September, was alerted to the issue, and opened the bug on March 6, 2024.

We continued to issue affected EV certificates after reporting the incident because we believed this to be an error or unintended discrepancy between the CA/Browser Forum's TLS Baseline Requirements and the Extended Validation Guidelines. Following feedback from the Bugzilla community, we fixed the certificates on March 18 and began notifying customers and revoking affected certificates. This mis-issuance affected 26,641 EV certificates. The incident and our response are described in bug #1883843.

Note: During our investigation of this issue, we noted that a subset of 1,975 EV certificates were also issued without the Entrust EV policy identifier (OID), based on our interpretation of the ballot update. This issue is described in bug #1888714.

Certificates missing serverAuth EKU (#1886467): The TLS Baseline Requirements also required certificates with extended key usage (EKU) to include both clientAuth and serverAuth EKUs; before the update clientAuth-only EKUs were permissible. The Entrust product platform allows subscribers to choose clientAuth, serverAuth or both. Entrust did not recognize that the change to the TLS Baseline Requirements required changes to this user interface product feature, and the associated linter and CPS. This caused mis-issuance of 1,176 certificates as described in bug #1886467.

CPS Updates: As we updated our EV Certificate profile to resolve bug #1883843, we made two oversights. First, we did not immediately update our CPS to reflect the changes made to the EV certificates on March 18; the issue was fixed in approximately three days. There were 9,045 certificates affected (aside from those already scheduled for revocation as part of bug #1883843), as described in bug #1887753.

Additionally, as we updated the CPS to add the CPS URI qualifier to the EV certificate profile, we inadvertently added this to the OV TLS certificate profile instead. While these certificates were issued in accordance with the TLS Baseline Requirements and our intended certificate profile, there were 6,008 OV certificates issued before the CPS was corrected, as described in bug #1890896.

2.1.2 Associated Bug List

Open Date	Bugzilla	Description
2024-03-06 2024-03-29	1883843 1888714	Missing EV CPS URI Missing EV Issuer Policy OID
2024-03-20	1886467	No serverAuth EKU
2024-03-25	1887753	Delay posting CPS for EV profile changes
2024-04-10	1890896	OV TLS CPS Typo Error

2.1.3 Root Cause Analysis

We misinterpreted the requirement to keep cPSuri in EV certificates, and initially chose not to revoke, believing that the EV Guidelines were in error. Change procedures did not include appropriate review and quality assurance to ensure that updates to TLS Baseline Requirements and EV Guidelines were followed. Additionally, we did not use linters that included the Ballot SC-62v2 changes; we could have used pkilint, which was only in pre-release at that time.

2.1.4 Improvement Plan

We are addressing root cause issues with an increased focus on compliance, change controls, and how we leverage linting technology, as outlined in the chart below.

Actions Items	Target Completion
PEOPLE	
Change organizational structure to enhance support, governance, and resourcing for compliance team	Complete
Engage external consultant to review compliance changes	Complete
Increase team assigned to execute CA/B Forum requirements and expectations	Complete
PROCESS	
Establish cross-functional change control board	Complete
Implement robust cross-functional change control process to cover full lifecycle planning and execution of changes for public trust certificates	2024-06-30
Create matrix of external standards for public-trust operations and products	2024-06-30
Implement Compliance by Design checklist to ensure requirements are considered at the inception of the design or design modification process	2024-06-30
Establish clearer naming conventions for certificate profiles to reduce potential errors	2024-07-31
TECHNOLOGY	
Deploy pkilint as a post-issuance linter for all public certs	Complete
Implement daily testing protocol to ensure efficacy of linters for public certificates	Complete
Update TLS BR EKU checking zlint	Complete
Expand use of linters post-issuance for all certificate types	Complete
Expand use of linters pre-issuance for all certificate types	2024-07-31

2.2 Incident Related to EV Locality Issue

2.2.1 Issue Description

EV certificates contain jurisdiction information (Locality, State, Country) that is derived from verified business registration information. Entrust issued some certificates with Locality populated (and Country populated) but missing State data. This missing State data was not in compliance with the EV Guidelines and constituted a mis-issuance of 106 certificates.

2.2.2 Associated Bug List

Open Date	Bugzilla	Description
2024-04-03	1897630	EV Locality Errors

2.2.3 Root Cause Analysis

Root causes of this mis-issuance are manual processes that enabled human error. Moreover, change procedures and quality processes did not include appropriate review for this issue.

2.2.4 Improvement Plan

We are addressing root causes with increased compliance resources, improved quality and change control processes, and more robust use of linting technology to prevent similar incidents.

Action Items	Target Completion
PEOPLE	
Change organizational structure to enhance support, governance, and resourcing for compliance team	Complete
PROCESS	
Establish cross-functional change control board	Complete
Implement robust cross-functional change control process to cover full lifecycle planning and execution of changes for public trust certificates	2024-06-30
Create matrix of external standards for public-trust operations and products	2024-06-30
Implement Compliance by Design checklist to ensure requirements are considered at the inception of the design or design modification process	2024-06-30
Review verification process for all certificate types	2024-06-30
TECHNOLOGY	
Deploy pkilint as a post-issuance linter for EV certs	Complete
Expand use of linters for other cryptographic or compliance objects	Complete

Action Items	Target Completion
Expand use of linters pre-issuance for all certificate types	2024-07-31
Implement additional input validation controls to prevent invalid combinations of jurisdiction fields	2024-07-31

2.3 Incident Handling/Communication

2.3.1 Issue Description

Key incidents in this area:

- **Delayed Response to CPR – EV Certificates missing cPSuri – Bug 1885754**
  Entrust received two Certificate Problem Reports (CPR), which per the TLS Baseline Requirements, must be responded to within 24 hours of receipt. We sent the response to the first CPR two hours after it was due and delivered the response to the second CPR two days after it was due. Subscribers were notified after we made the revocation decision.

- **Delayed Posting of Incident Reports – Bugs 1890123, 1890901, 1898847**
  Section 4.9.5 of the TLS Baseline Requirements requires that we provide a preliminary incident report to subscribers and the entity that reported the issue within 24 hours. For the missing cPSuri issue, we provided a preliminary incident report in 43 hours. A second reporter was told where they could find the preliminary incident report, but we did not attach a copy or a direct link to that communication.

We filed the incident report for the CPS typographic error 15 days late.

The Mozilla Root Store Policy says that incident reports should be filed within 72 hours of confirmation and full reports within two weeks of confirmation. For the Jurisdiction issue, the incident was observed on April 15 but not investigated and confirmed until May 16. The incident report was filed within 72 hours of confirmation on May 16, but should have been escalated for investigation and confirmation on April 15 versus May 16 and, therefore, filed closer in time to the discovery and with earlier notice to subscribers.

2.3.2 Associated Bug List

Open Date	Bugzilla	Description
2024-03-16	1885754	Delayed Response to CPR (24hrs)
2024-04-06 2024-04-10 2024-05-24	1890123 1890901 1898847	Delayed Posting Incident Reports (72hrs)

2.3.3 Root Cause Analysis

The common root cause of these issues is an incident handling and response procedure that required more clarity in required actions, roles, and responsibilities. In addition, incoming CPRs were mixed in with other incoming support cases. While this has not been an issue in the past,

in the Jurisdiction issue, it contributed to human error in identifying and prioritizing CPRs versus support cases. As a result, these problem reports were either not escalated for investigation or not communicated externally in a timely manner.

2.3.4 Improvement Plan

Entrust will create an end-to-end CPR incident response plan that leverages the best-practices model used by our Information Security team. This formal response plan will ensure internal reports and external CPRs are quickly identified and escalated to the right teams for handling and management.

The plan also will use automation and tracking mechanisms to help ensure that incident reports, communications to reporters and subscribers, and responses to comments on the Bugzilla forum are posted and responded to in accordance with the CA/Browser Forum requirements and the Root Embedding Programs.

Action Items	Target Completion
PEOPLE	
Change organizational structure to ensure adequate support and resourcing for compliance team	Complete
PROCESS	
Implement formal incident response process including incident response communication plan to meet mandatory reporting times	2024-06-30
Implement specific handling processes for internal as well as external (CPR) reports	2024-06-30
TECHNOLOGY	
Implement flag for CPRs coming into Support case management system	2024-08-31
Automate CPR form to collect all required information at the outset from the reporter rather than relying solely on email	2024-08-31

2.4 Operational Updates

2.4.1 Issue Description

One of the reporters of the EV cert issue alerted Entrust that the Problem Reporting Mechanism in its CCADB entry was misaligned with its CPS and contained outdated information (bug 1894111). The contact email was ecs.support@entrustdatacard.com when it should have been ecs.support@entrust.com (as reflected in the CPS).

Entrust Datacard changed its name to Entrust on September 14, 2020, and the ECS Support email address changed from @entrustdatacard.com to @entrust.com. The entrustdatcard.com address remains functional and automatically forwarded to the new address. As a result, all CPRs were received as intended. That said, this highlights the need to regularly review and confirm this information.

For bug 1879602, two root CA OCSP responders were signed using SHA-1 when SHA-256 was required by Section 7.1.3.2.1 of the TLS Baseline Requirements.

Regarding bug 1889217, Entrust posted 2 CRLs to the CCADB that did not meet RFC standard format.

2.4.2 Associated Bug List

Open Date	Bugzilla	Description
2024-04-29	1894111	Failure to update CCADB Fields
2024-02-09	1879602	OCSP SHA1 Signatures
2024-04-02	1889217	CRL Format Error

2.4.3 Root Cause Analysis

These issues were caused by insufficient change control processes. We are updating processes and related documentation to improve moving forward. For specific incidents:

- Entrust regularly updates the CCADB information to address CPS updates, CA certificate generation, CA certificate revocation, annual audit updates, annual self-assessment updates, and test sites. However, the static information on the CCADB CA OWNER page where the Problem Reporting Mechanism is found was not reviewed consistently, and we should have updated this with our corporate domain change.

- The default configuration for our OCSP responders is to sign with the algorithm which was used to sign the CA certificate. A year before the OCSP SHA-1 sunset date, the offline root components were updated to sign with SHA-256. The online OCSP responders for those legacy SHA-1 CAs were not updated, so they did not meet the eventual OCSP SHA-1 sunset date.

- The CRL generation software relies on a function within the official Go core, which we forked into a separate private library. There was a bug in the library that was fixed by the community, however the fix was created in a separate version to keep the compatibility contract. The library used in our CRL component was dated after the fix, but before the community posted a deprecation notice and so continued to use the faulty implementation.

2.4.4 Improvement Plan

All three of these incidents were quickly remediated. Entrust has formalized its process around CCADB updates to ensure that all information, including the CA Owner page, stays accurate and up to date. That written process delineates clear lines of responsibility and the cadence for reviewing information and providing updates. Linting of all cryptographic objects, including CRLS and OCSP responses, should prevent recurrences of the OCSP and CRL format issues.

Action Items	Target Completion
PROCESS	
Review and update CCADB policy to ensure inclusion of CA owner page	Complete
TECHNOLOGY	
Run pkilint against all CRLs	Complete
Update CRL generation software installed for online and offline CRL systems. Issue and publish CRLs	Complete
Update automated test to cover the added requirement	Complete
Set up plan for periodically reviewing forked libraries. Release note patches.	Complete
Reconfigure OCSP responders to sign with SHA-256 and add OCSP Watch to daily monitoring	Complete

2.5 Delayed Revocation

2.5.1 Issue Description

Entrust filed delayed revocation bugs as we addressed the EV TLS certificates with missing cPSuri (bug 1886532) and clientAuth TLS without serverAuth EKU (bug 1887705).

The TLS Baseline Requirements state that CAs must revoke mis-issued certificates within five days in an incident that does not compromise security. There were two delays in the EV certs missing cPSuri incident:

1. Entrust initially continued issuing the affected EV certificates and postponed subscriber notification and revocation, believing that the misalignment between TLS Baseline Requirements and the EV Guidelines was an error or unintended oversight of Ballot SC-62v2, and that the issue merited discussion prior to making a revocation decision.

2. Once we declared the mis-issuance we quickly notified customers. We received significant subscriber pushback on the revocation deadlines due to negative impact on their critical operations.

The Mozilla Root Store Policy specifies that when revocation is delayed at the request of specific subscribers, the rationale must be provided on a per-subscriber basis. Any decision to not comply with the timeline specified in the Baseline Requirements must also be accompanied by a clear timeline describing if and when the problematic certificates will be revoked or expire naturally and supported by the rationale to delay revocation.

In both incidents, delayed revocation was granted to subscribers who submitted specific requests for exceptions, primarily on the basis of avoiding disruption to critical operations.

As of May 30, 2024, at 19:29 UTC, all affected clientAuth certificates (bug #1886467) were revoked. As of June 7, 2024, all certificates related to the EV Certificate issue (bugs 1883843 and 1888714) have been revoked.

Note: We also posted a third delayed revocation bug for the Jurisdiction issue (see bug #1898848). We revoked and re-issued all affected certificates within five days after the mis-issuance was confirmed. Our investigation found that we should have actioned this issue earlier, so we filed an incident (bug #1898848) based on the time when the incident should have been confirmed.

2.5.2 Associated Bug List

Open Date	Bugzilla	Description
2024-03-20	1886532	Delayed Revocation for missing cPSuri in TLS EV Certs
2024-03-25	1887705	Delayed Revocation clientAuth TLS certs w/o serverAuth EKU
2024-05-24	1898848	Delayed Revocation for Jurisdiction Locality Error

2.5.3 Root Cause Analysis

Entrust initially did not believe revocation was required for the missing cPSuri issue and was already beyond the five-day period when it reversed that position and began revoking and re-issuing.

We continued issuing the EV certificates with the missing cPSuri because we believed there was an unintended discrepancy between the TLS Baseline Requirements and the EV Guidelines, and wanted to avoid disruption to the web ecosystem, hoping that we could resolve the discrepancy with the CA/Browser Forum.

Across all incidents, significant subscriber pushback to the five-day revocation timeline followed due to perceived disruption of critical operations. Many subscribers have automation in place, but regulations and complex partner ecosystems prevented them from acting within the required timeframes. Taking this into account, we worked with subscribers individually to plan and map revocation timelines, which at times extended past the five-day requirement.

When we addressed delayed revocation in 2020, we made several statements regarding how we would avoid delayed revocation in the future. We have continued to educate our subscribers regarding the need for greater agility and resilience, but we did not make the progress necessary to enable five-day revocation without large-scale disruption to their critical operations. Based on this root cause analysis, we believe the improvement plan below will address the issues identified.

2.5.4 Improvement Plan

We agree that it is critical for CAs to be prepared to follow revocation requirements in the TLS Baseline Requirements and we intend to follow the rules set out by the trusted root programs.

Entrust has the technical capability to meet the 24-hour and 5-day revocation requirements. We are engaging with our subscribers to help them meet these requirements moving forward with minimal disruption.

The improvement plan includes:

- **Compliance**: We intend to revoke and replace certificates that do not meet TLS Baseline Requirements or certificate-specific guidelines. We will plan to do so within the prescribed revocation periods. We will work with our subscribers to ensure awareness and minimize delayed revocation requests; such requests will be handled only on a case-by-case basis, and only under limited circumstances. We will have this plan in place by the end of June.

- **Policy Updates**: We ensure that policies are updated and that they are communicated to subscribers. We are considering ways to increase visibility of the CA's right to revoke certificates on short notice beyond our contract language. We also will add a warning to manual order pages and related emails to ensure subscriber understanding of required timelines.

- **Advancing ACME:** We are supporting the ongoing work to automate certificate issuance and management. Entrust experts have authored two IETF drafts around ACME auto discovery, which will help to increase automation adoption by subscribers using public certificates.

- **Driving customer adoption of automation:** We believe automation is critical to enable ongoing resilience**.** We have begun campaigns to urge subscribers to adopt automation solutions from Entrust or other providers, including offering our CertHub certificate lifecycle management tool for 12 months at no charge. We are looking at additional ways to drive customer adoption of solutions that enable them to minimize disruption in the event of a five-day or 24-hour revocation.

- **Leveraging ARI:** We plan to implement ACME Renewal Information (ARI) capabilities into the Entrust platform, and to add similar capabilities into our REST APIs. These capabilities will allow clients to automate renewal in response to future revocation events.

In addition, we are taking measures to strengthen our internal policies and controls around revocation, as reflected in the table below.

Action Items	Target Completion
PROCESS	
Create formal revocation event handling process	2024-06-30
Establish delayed revocation criteria	2024-06-30
Create revocation event communication plan	2024-06-30
Launch communication and education to subscribers on requirements for public trust certificates	2024-07-31
TECHNOLOGY	
Implement ACME ARI	2024-07-31

Action Items	Target Completion
Implement ARI capabilities via API to integrate with clients that use our API	2024-07-31

3. Conclusion

As we said at the outset of this report, we set high standards for ourselves, and recognize that these incidents were unnecessary and based on our own mistakes or misjudgments. We have thoughtfully considered your questions and comments on these issues, and this input is reflected in our plans.

This report is the result of a thorough review of the root causes of these incidents. Our action plans (see Appendix 2) demonstrate how Entrust will manage compliance with the TLS Baseline Requirements, applicable root program policies, and community expectations.

We have identified the necessary resources and have support at the highest levels of our organization to ensure accountability and execution on these plans.

Entrust takes this responsibility seriously and is committed to the security and resilience of the web ecosystem.

Appendix 1: Full Bug List

Open Date	Bugzilla	Description
Incidents Related to Ballot SC-62v2 and EV Locality Issue		
2024-03-06 2024-03-29	1883843 1888714	Missing EV CPS URI Missing EV Issuer Policy OID
2024-03-20	1886467	No serverAuth EKU
2024-03-25	1887753	Delay posting CPS for EV profile changes
2024-04-10	1890896	OV TLS CPS Typo Error
2024-04-03	1897630	EV Locality Errors
Incident Handling/Communication		
2024-03-16	1885754	Delayed Response to CPR (24hrs)
2024-04-06 2024-04-10 2024-05-24	1890123 1890901 1898847	Delayed Posting Incident Reports (72hrs)
2024-03-20 2024-03-25 2024-05-24	1886532 1887705 1898848	Delayed Revocation for missing cPSuri in TLS EV Certs Delayed Revocation clientAuth TLS certs w/o serverAuth EKU Delayed Revocation for Jurisdiction Locality Error
Operational Changes		
2024-04-29	1894111	Failure to update CCADB Fields
2024-02-09	1879602	OCSP SHA1 Signatures
2024-04-02	1889217	CRL Format Error

Appendix 2: Improvement Measures

Action Items	Kind	Target Completion
PEOPLE		
Change organizational structure to enhance support, governance, and resourcing for compliance team	Prevent	Complete
Engage external consultants to review compliance changes	Prevent	Complete
Increase team assigned to execute CA/B Forum requirements and expectations	Prevent	Complete
PROCESS		
Establish cross-functional change control board	Prevent	Complete
Review and update CCADB policy to ensure inclusion of CA owner page.	Prevent	Complete
Implement robust cross-functional change control process to cover full lifecycle planning and execution of changes for public trust certificates	Prevent	2024-06-30
Create matrix of external standards for public-trust operations and products	Prevent	2024-06-30
Implement Compliance by Design checklist to ensure requirements are considered at the inception of the design or design modification process	Prevent	2024-06-30
Implement formal incident response process including incident response communication plan to meet mandatory reporting times	Prevent	2024-06-30
Implement specific handling processes for internal as well as external (CPR) reports	Prevent	2024-06-30
Review verification process for all certificate types	Prevent	2024-06-30
Create formal revocation event handling process	Prevent	2024-06-30
Establish delayed revocation criteria	Prevent	2024-06-30
Create revocation event communication plan	Prevent	2024-06-30
Launch communication and education to subscribers on requirements for public trust certificates	Prevent	2024-07-31
Establish clearer naming conventions for certificate profiles to reduce potential errors	Prevent	2024-07-31
TECHNOLOGY		
Run pkilint against all CRLs	Detect	Complete
Update CRL generation software installed for online and offline CRL systems. Issued and published CRLs.	Correct	Complete

Action Items	Kind	Target Completion
Update automated test to cover the added requirement.	Prevent	Complete
Set up plan for periodically reviewing forked libraries. Release note patches.	Detect	Complete
Reconfigure OCSP responders to sign with SHA-256 and added OCSP Watch to daily monitoring.	Detect	Complete
Implement daily testing protocol to ensure efficacy of linters for public certificates	Mitigate	Complete
Deploy pkilint as a post-issuance linter for EV certs	Detect	Complete
Update TLS BR EKU checking zlint	Mitigate	Complete
Expand use of linters for other cryptographic or compliance objects	Detect	Complete
Expand use of linters post-issuance for all certificate types	Detect	Complete
Expand use of linters pre-issuance for all certificate types	Detect	2024-07-31
Implement ACME ARI	Mitigate	2024-07-31
Implement additional input validation controls to prevent invalid combinations of jurisdiction fields	Mitigate	2024-07-31
Implement ARI capabilities via API to integrate with clients that use our API	Mitigate	2024-07-31
Implement flag for CPRs coming into Support case management system	Prevent	2024-08-31
Automate CPR form to collect all required information at the outset from the reporter rather than relying solely on email	Prevent	2024-08-31