|  |
| --- |
| **Audit Name: 20149**  **Audit Number: Novologix Integration with Aetna Systems** |

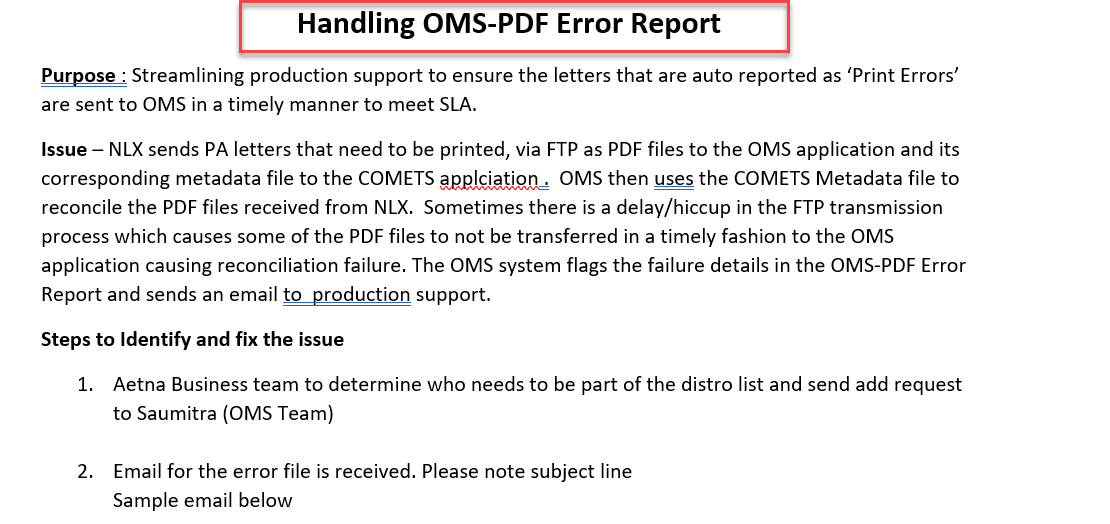
|  |  |
| --- | --- |
| Control & Sample Information | |
| Control | 20149 – Novologix Integration with Aetna Systems |
| Sample Number | 4 out of 15 CUECs. CUEC#3,4,13 &15 |
| Supporting Documentation Received From | Brian Tuberty Dir. IT Program Management |
| Received Date | 12/23/2020, 01/15/2021, and 01/27/2021 |
| Purpose of the Test | The purpose of this test is to mitigate risk for systems involved in the integration efforts between Novologix and HCB systems. |
| Source Files | [CUEC Number 3- Handling OMS-PDF error file (1).docx](https://cvshealth.auditboardapp.com/download?file_id=57729) 12/23/2020  [CUEC Number 3- OMSPDF Error Report.msg](https://cvshealth.auditboardapp.com/download?file_id=57730) 12/23/2020  [CUEC Number 4- SFTP File Transmission Request(CE).msg](https://cvshealth.auditboardapp.com/download?file_id=58442) 01/27/2021  [CUEC Number 4- SFTP Setup Questionnaire -Aetna B2b.docx](https://cvshealth.auditboardapp.com/download?file_id=60300) 02/04/2021  [CUEC Number 4SFTP Questionnaire Document. Meeting.ics](https://cvshealth.auditboardapp.com/download?file_id=60302) 02/04/2021  [CUEC Number 4-Migration Complete- Know Before You GoB2B Gateway.msg](https://cvshealth.auditboardapp.com/download?file_id=60303) 02/04/2021  [CUEC Number 4-SFG PROD The Deployment Activity is Successful.msg](https://cvshealth.auditboardapp.com/download?file_id=60304) 02/04/2021  [CUEC Number 13 – Employee Training.docx 01/28/2021](https://cvshealth.auditboardapp.com/download?file_id=60301&name=Employee%20Training.docx)  [CUEC Number 13 - CHIP-0020 - CVS Health Corporate Breach Notification Policy and Procedure](https://cvshealth.auditboardapp.com/download?file_id=60299&name=CUEC%20Number%2013-CHIP-0020%20-%20CVS%20Health%20Corporate%20Breach%20Notification%20Policy%20and%20Procedure.pdf) 02/03/2021  [CUEC Number 13 - CIST-0056 - Application Security Standard](https://cvshealth.auditboardapp.com/download?file_id=60295&name=CUEC%20Number%2013-CIST-0056%20-%20Application%20Security%20Standard.pdf) 02/03/2021  [CUEC Number 15 – Novologix All Defect Dump file.xlsx](https://cvshealth.auditboardapp.com/download?file_id=58271&name=CUEC%20Number%2015%20-%20Novologix%20All%20Defect%20Dump%20-%20Feb20%20-%20Nov20.xlsx) 01/15/2021  [CUEC Number 15 – Post Install Triage – Email Thread.msg](https://cvshealth.auditboardapp.com/download?file_id=58270&name=CUEC%20Number%2015%20-%20Post%20Install%20Traige%20-%20Email%20Thread%20ITPR041816ITPR042956%20AI%20BI%20Claims%20Editing.msg) 01/15/2021 |

**Attribute 1:** Management has considered and implemented in-scope CUEC’s identified within the Novologix SOC1 report related to Claims Editing and Prior Authorization initiative.

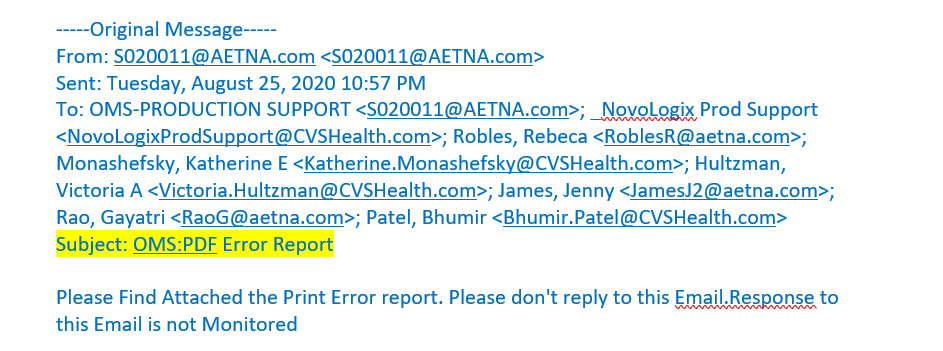
**Sample 3, CUEC #3(Claims Editing & Prior Authorization)**: User entities monitor transmissions to Novologix and take corrective action on errors identified during the file submission process.

IA received artifacts derived out of 2 document requests (#4165 and #4327) from Brian Tuberty, Dir. IT Program Management on 12/23/2020. On 12/23/2020,

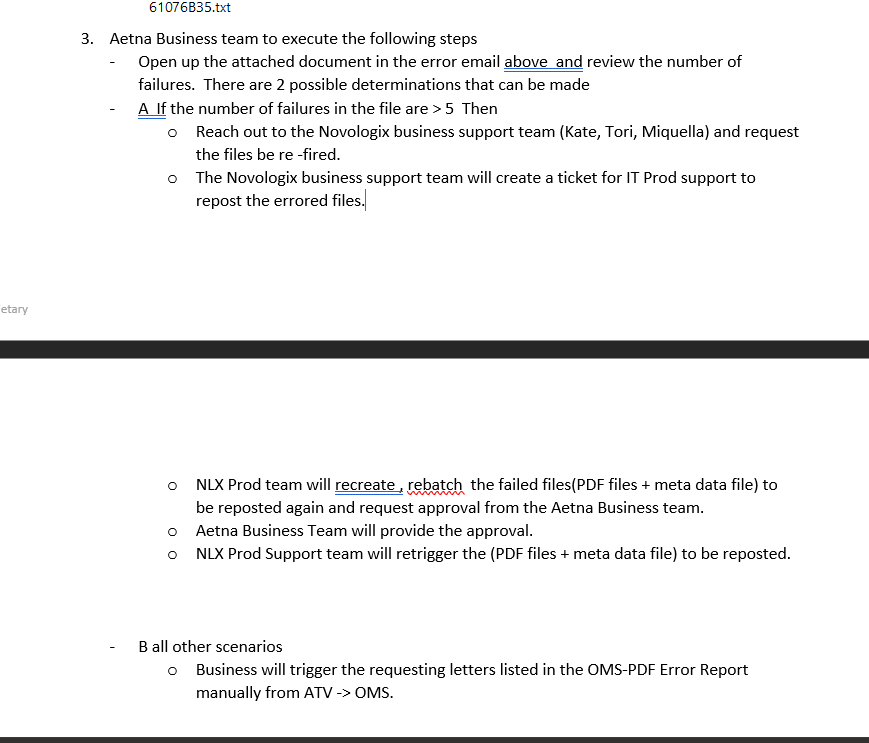
IA received from Brian Tuberty, Dir. IT Program Management. A word document explaining the workflow/process the team takes in receiving errors and rectifying them from both a claims editing and prior authorization perspective. (See [CUEC Number 3- Handling OMS-PDF error file (1).docx](https://cvshealth.auditboardapp.com/download?file_id=57729)). The document lists the workflow included in the escalation process, and what an identified error email would look like.



IA noted in the document received from Tuberty that team members have a process in place for handling error reports.

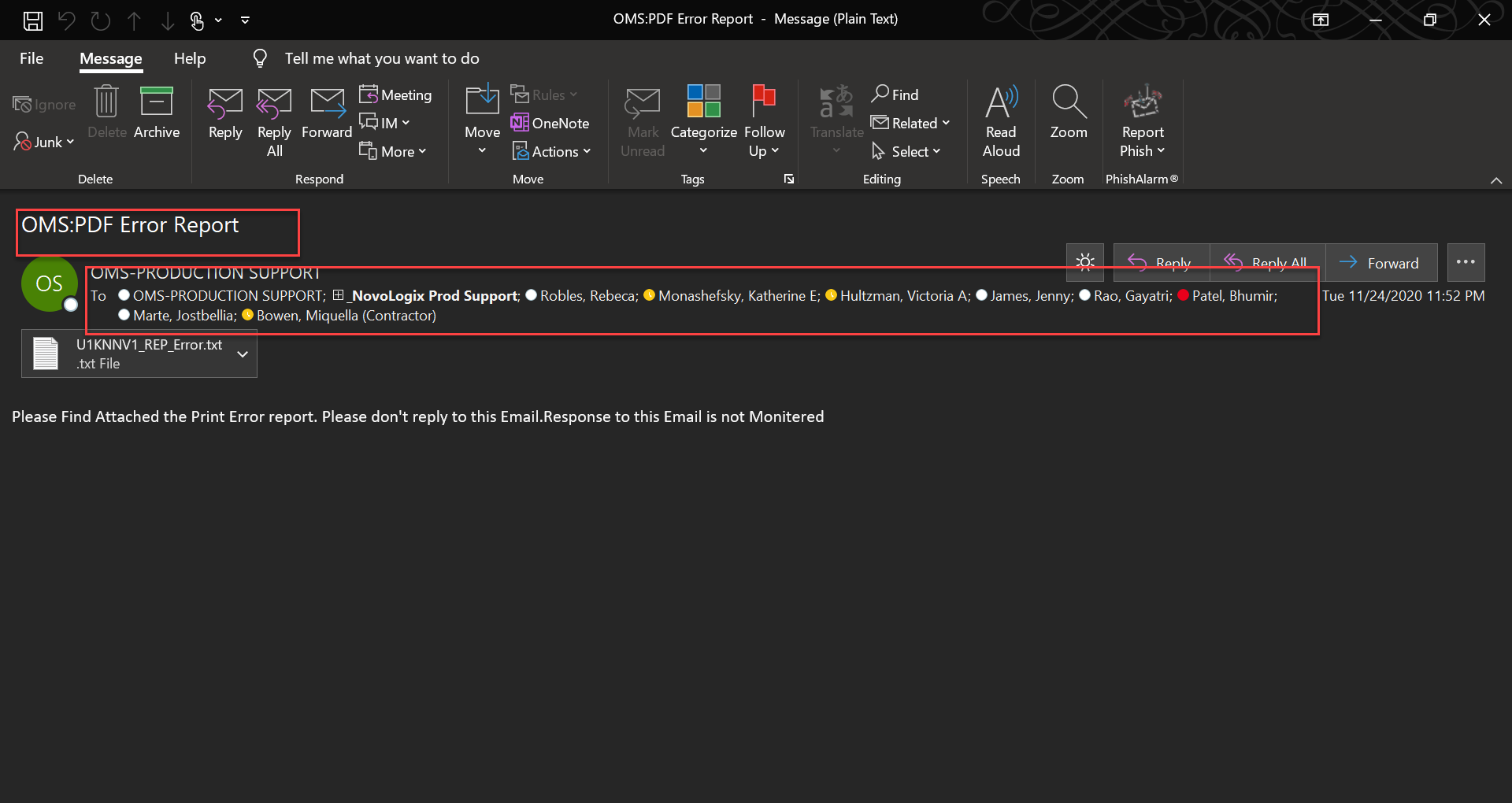


On page 1, paragraph 5, an example of an error report being sent to the team for review.



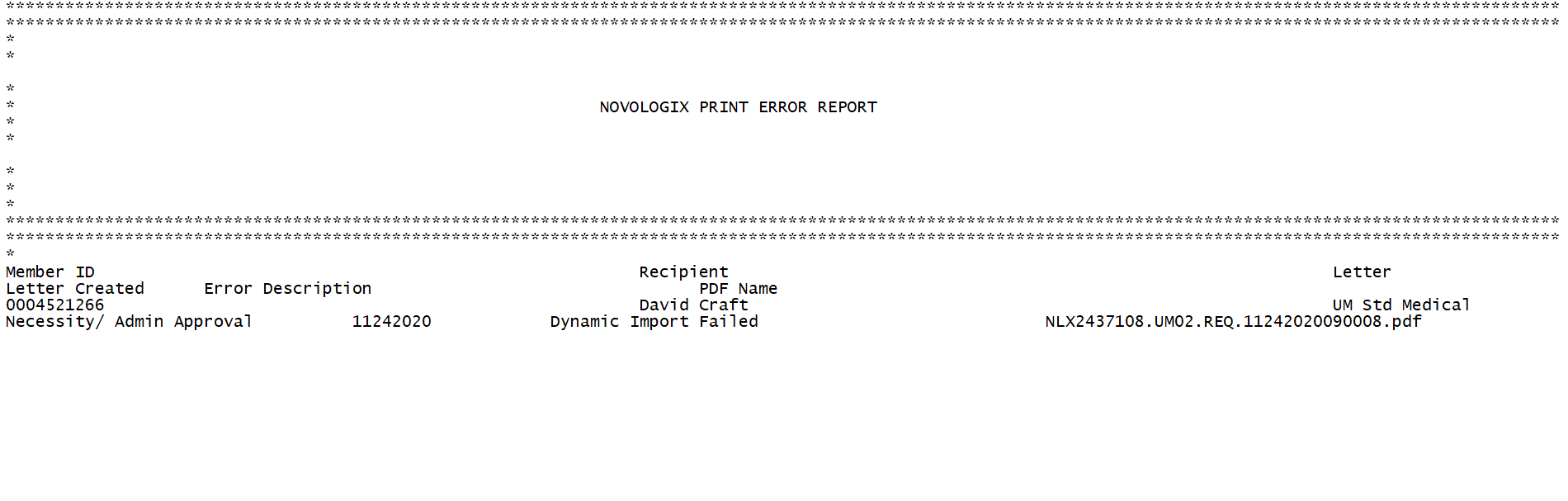
On page 1, paragraph 8, a listed-out workflow illustrating the steps taken for handling identified errors.

On 12/23/2020, IA also received from Brian Tuberty, Dir. IT Program Management an example of an error sent to the team members (See [CUEC Number 3- OMSPDF Error Report.msg](https://cvshealth.auditboardapp.com/download?file_id=57730)). In this screenshot, IA observed an error report being sent to relevant team members for review.



IA observed an example of an error report being sent to relevant team members for review.

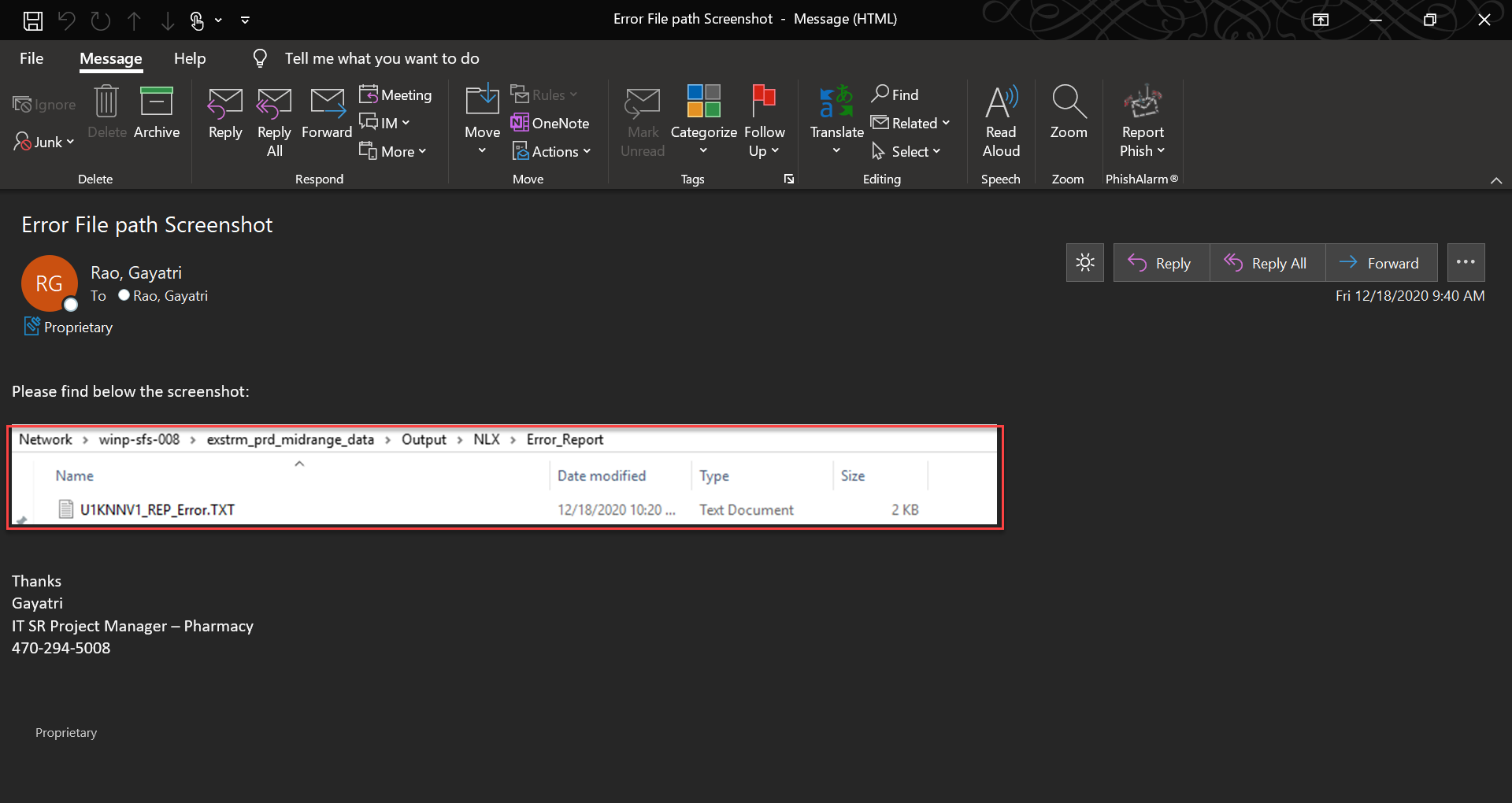
On 12/23/2020 IA received 3 examples of error reports from Brian Tuberty, Dir. IT Program Management (See [CUEC Number 3- OMSPDF Error Report.msg](https://cvshealth.auditboardapp.com/download?file_id=57730) , [CUEC Number 3- U1KNNV1\_REP\_Error (6).txt](https://cvshealth.auditboardapp.com/download?file_id=57731) and [CUEC Number 3-Error File path Screenshot.msg](https://cvshealth.auditboardapp.com/download?file_id=57732)) These examples show that errors are being monitored to perform the necessary escalation process.



An example of a Novologix error report.



Another example of a Novologix error report.

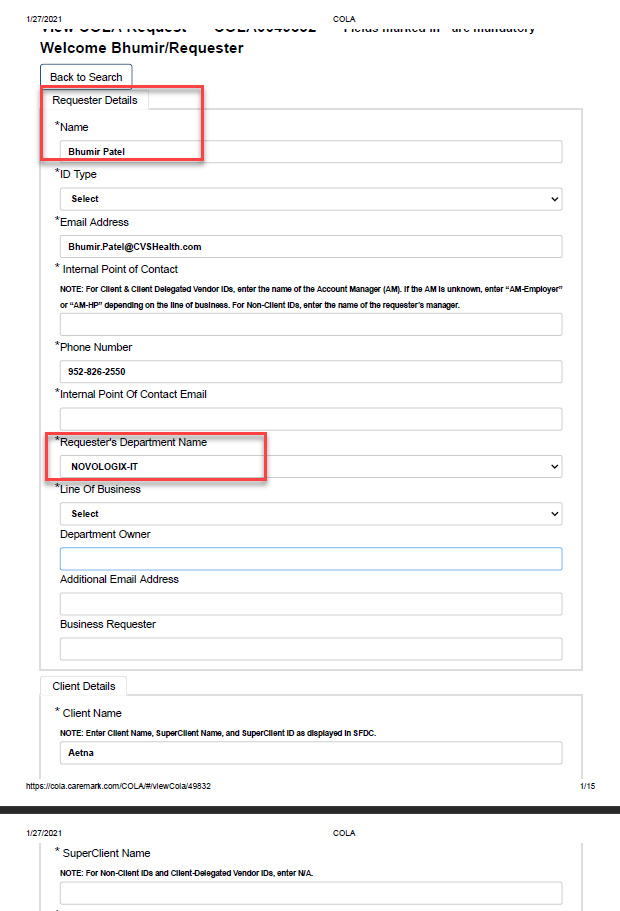


An example of a Novologix error report that also illustrates where the error was from and the path of the error.

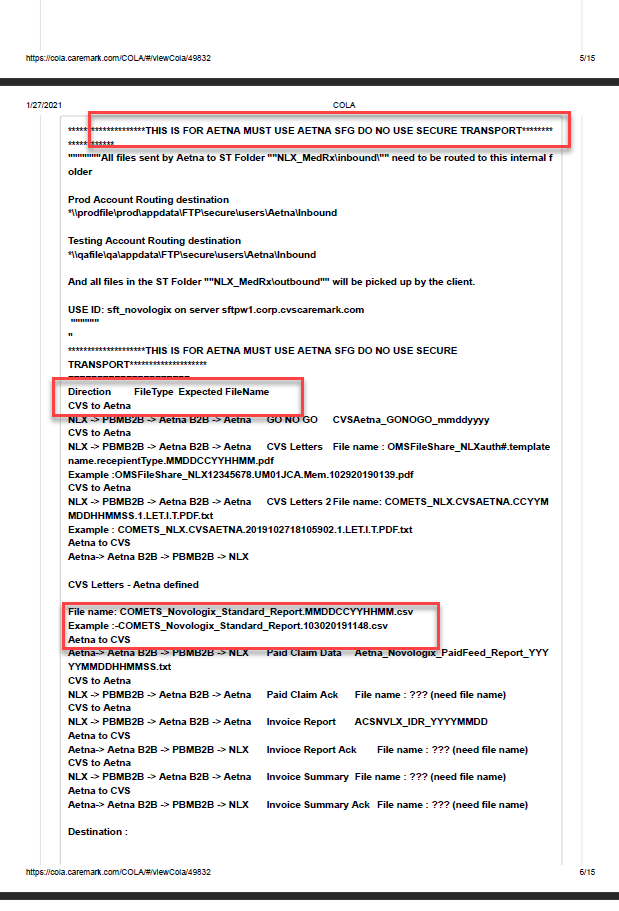
Attribute satisfied.

**Sample 4, CUEC #4 (Claims Editing):** User entities are responsible for internally securing the data files transmitted to and received from Novologix.

On 1/27/2021 IA received an SFTP file request form made by Bhumir Patel, Advisor, App. Development, Novologix IT from Brian Tuberty, Dir. Application Development (See [CUEC Number 4- SFTP File Transmission Request(CE).msg](https://cvshealth.auditboardapp.com/download?file_id=58442)). In this document, a request for a file transport is observed. IA observed evidence that files are transmitted securely from a Claims Editing perspective. Yet, IA also observed that instead of using SFTP, the transmission is being done using SFG. During a quick google search, IA discovered that “SFG” stands for “Sterling File Gateway”.

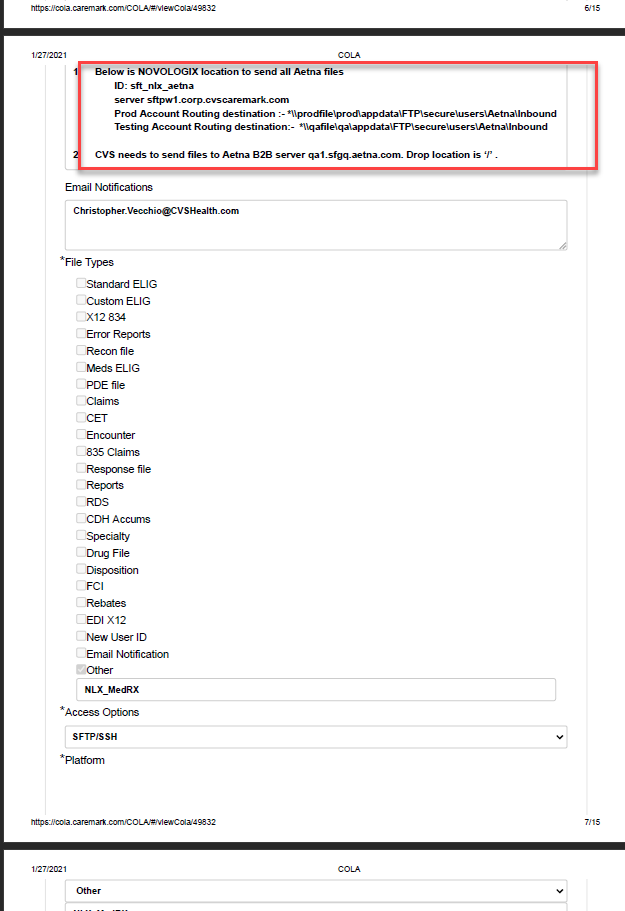


On page 1 of the request form, IA observed the requester of this file transmission request was Bhumir Patel, Adv. App. Development, Novologix IT.

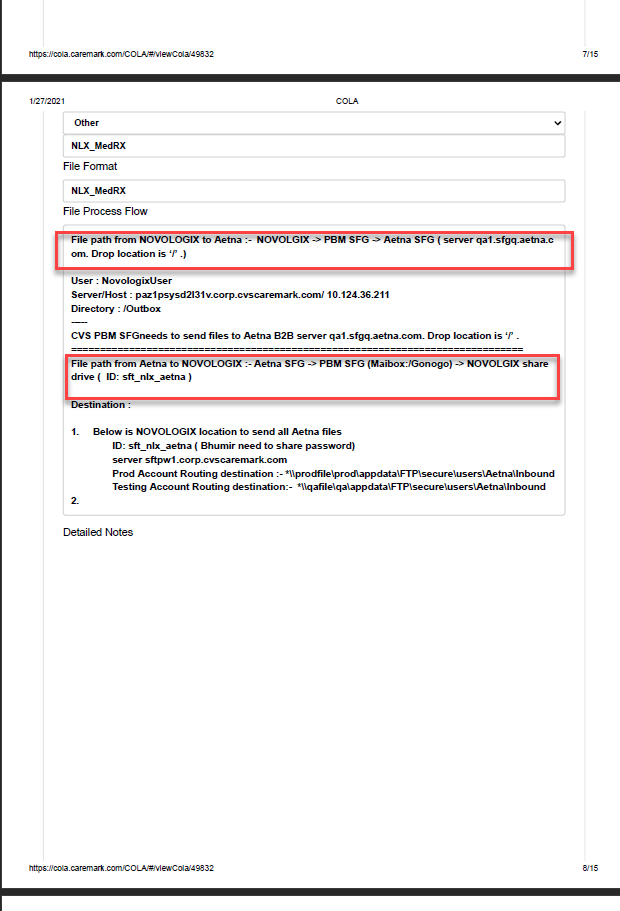


IA observed on page 6 of request; the file being transmitted and the expected destinations.

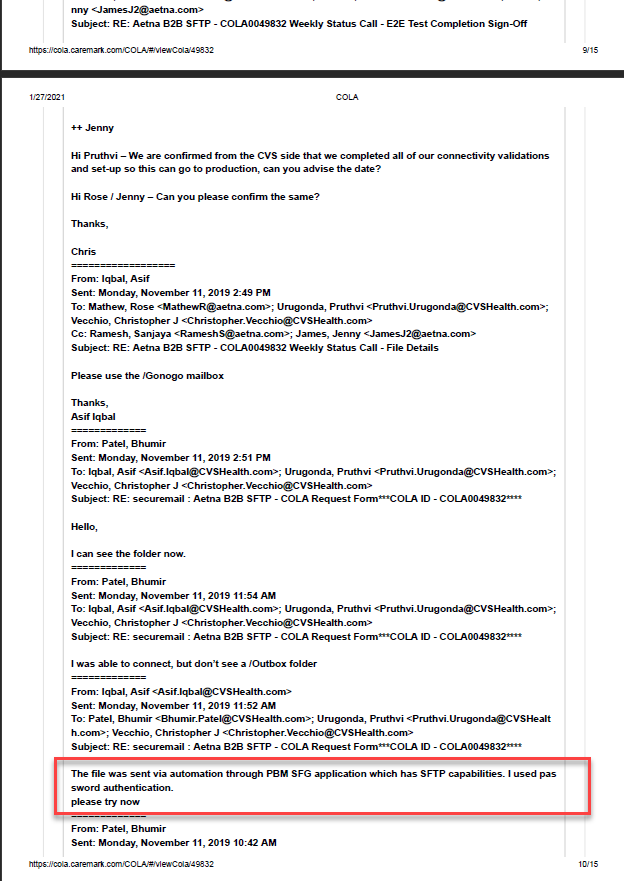
On page 6, a note on the request form that alludes to the required usage of SFG instead of SFTP.



IA observed on page 7 the “sftp” server being used during this process.

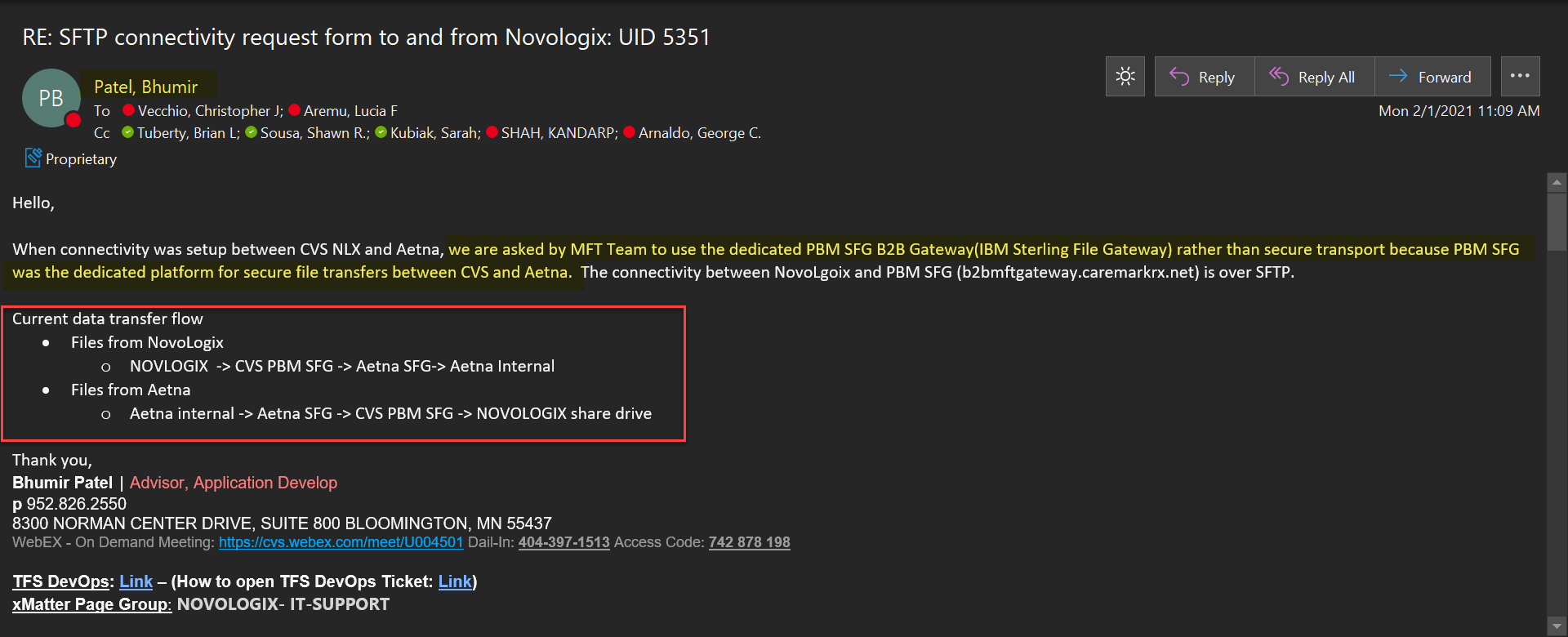


On page 8 of the request form; The file path for this transmission is shown here to be using “SFG” during this process.



Page 10 of the document, communication from Iqbal Asif, Sr. Adv. Application Development Data Mgmt. to Bhumir Patel, Adv. App. Development, Novologix IT, explaining that the file was sent using “SFG” instead of “SFTP”.

When asked why the file transmissions were occurring via SFG instead of SFTP (See [CUEC 4- SFTP vs SFG question to client-UID 5351.msg](https://cvshealth.auditboardapp.com/download?file_id=59236)), Bhumir Patel, Advisor, App. Development, Novologix IT, provided IA with an explanation.

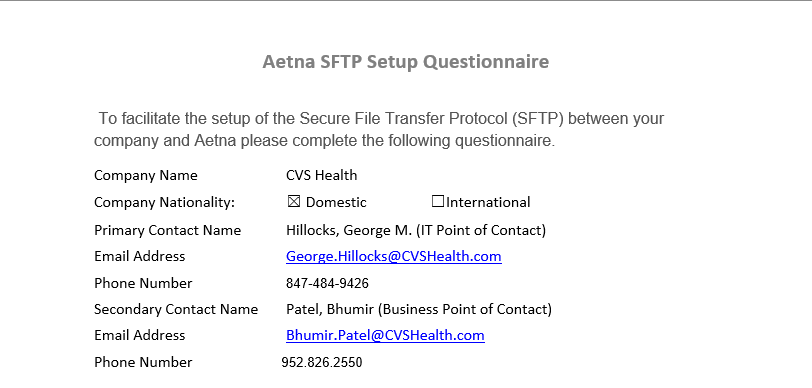


Patel explained that SFG was being used for transmitting files from Novologix CVS to Aetna and vice versa. Patel explains that this process is an institutional practice for the purposes of CVS and Aetna. He also illustrates the path of how files are being transferred to Aetna and from CVS Novologix.

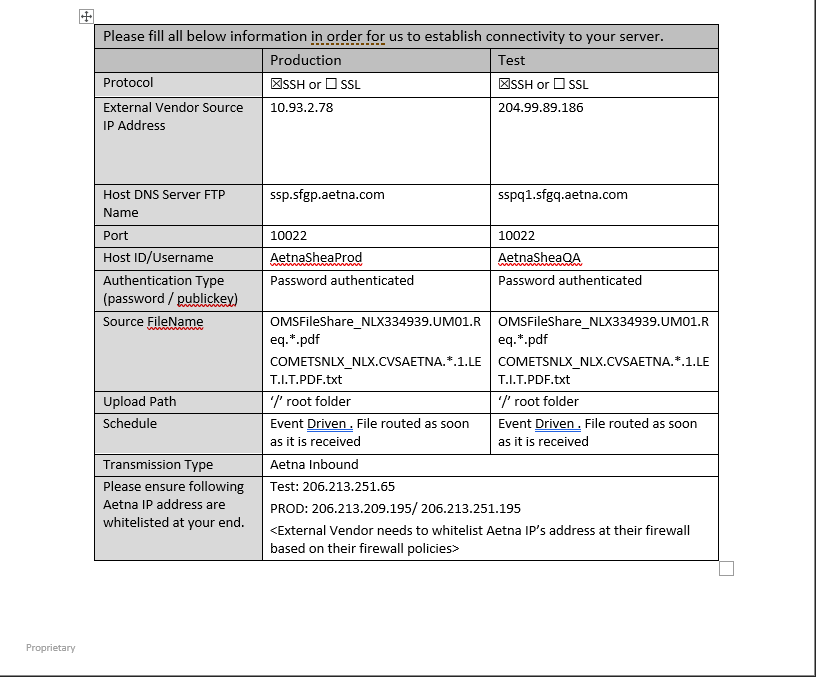
Attribute satisfied.

**Sample 4, CUEC #4 (Prior Authorization):** User entities are responsible for internally securing the data files transmitted to and received from Novologix.

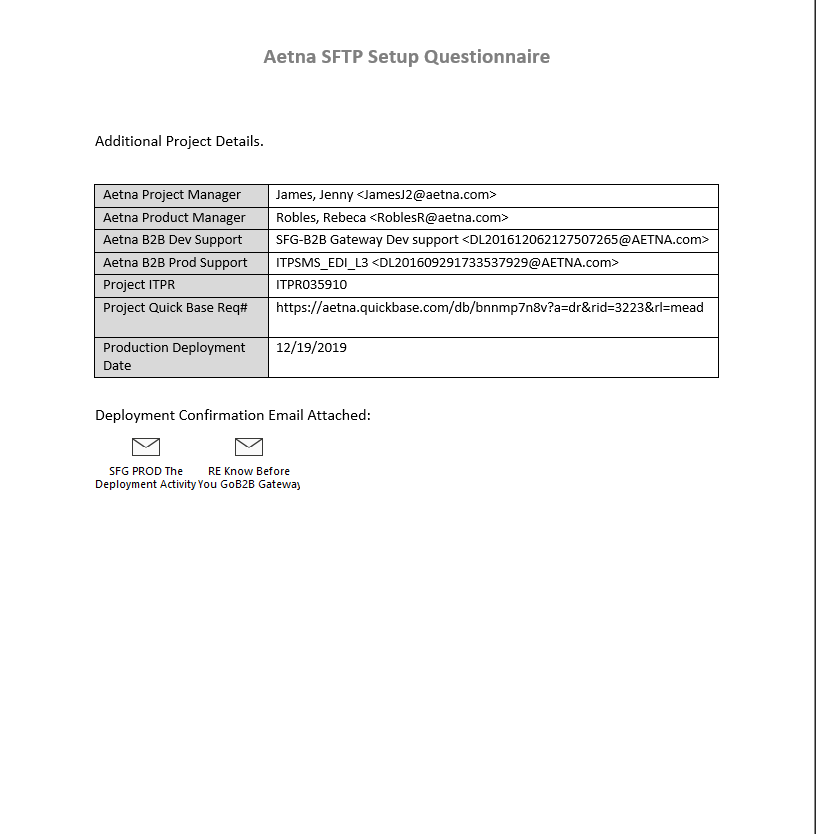
On 02/04/2021, IA received from Brian Tuberty an SFTP Questionnaire form that is utilized for transmitting Prior Authorization letters to Comet from Novologix (See [CUEC Number 4- SFTP Setup Questionnaire -Aetna B2b.docx](https://cvshealth.auditboardapp.com/download?file_id=60300)). In this document, IA observed a filled-out form depicting a file transfer using the SFG server. During a follow up meeting (See [CUEC Number 4SFTP Questionnaire Document. Meeting.ics](https://cvshealth.auditboardapp.com/download?file_id=60302)) with Gayatri Rao, IT Sr. Project Manager, Sanjaya Ramesh, App. Software Delivery Advisor, and Rose Mathew, Sr. App. Dev. IA learned that this questionnaire is utilized by the Aetna gateway team (Mathew and Ramesh) to transmit prior authorization letters written in files to be sent to Comet. During this meeting, Ramesh and Mathew offered IA an in-depth explanation of the document explaining the protocols, IP addresses, password authentication, the path of which the file is being sent and uploaded, and the schedule.



Page 1; The primary contact information of individuals on the CVS Novologix team responsible for sending out these questionnaires.

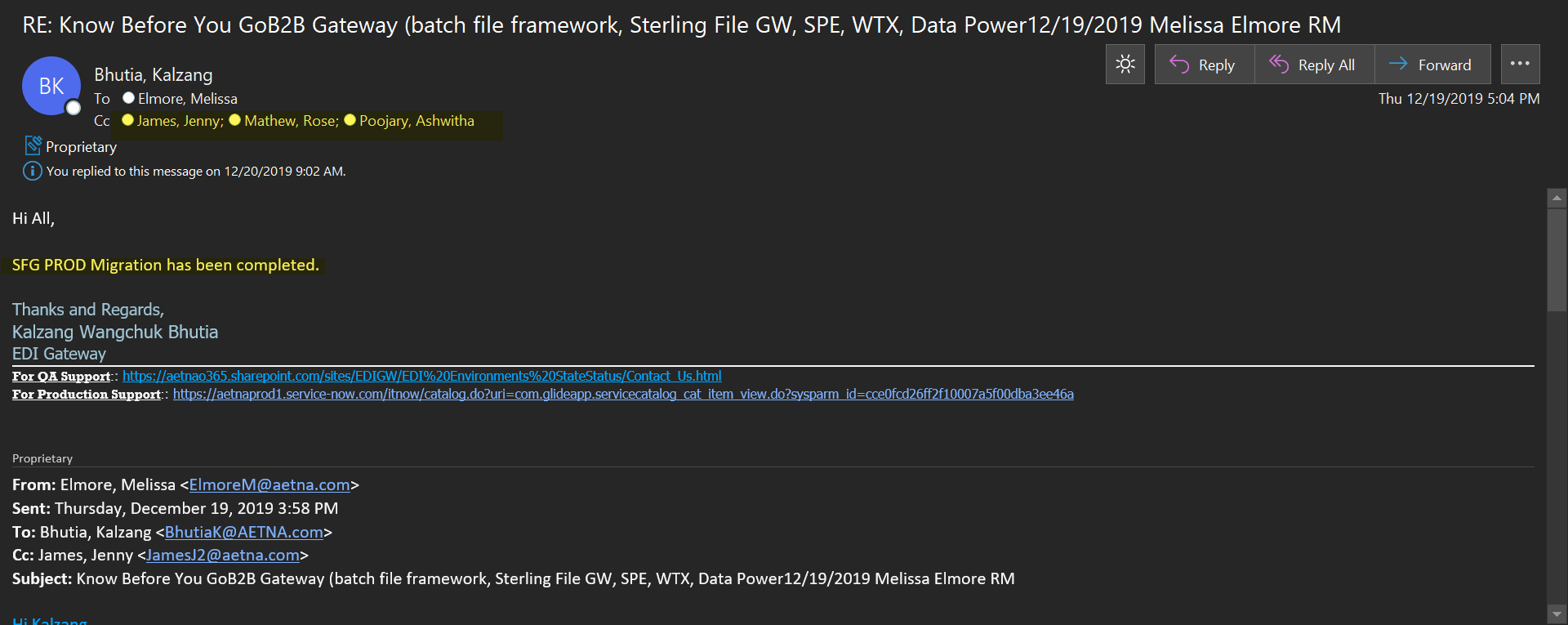


On page 1 of the questionnaire; the process for prior authorization file transfers. IA observed the form depicts the IP address being used, the servers being used, host name, authentication method, and the file in question.

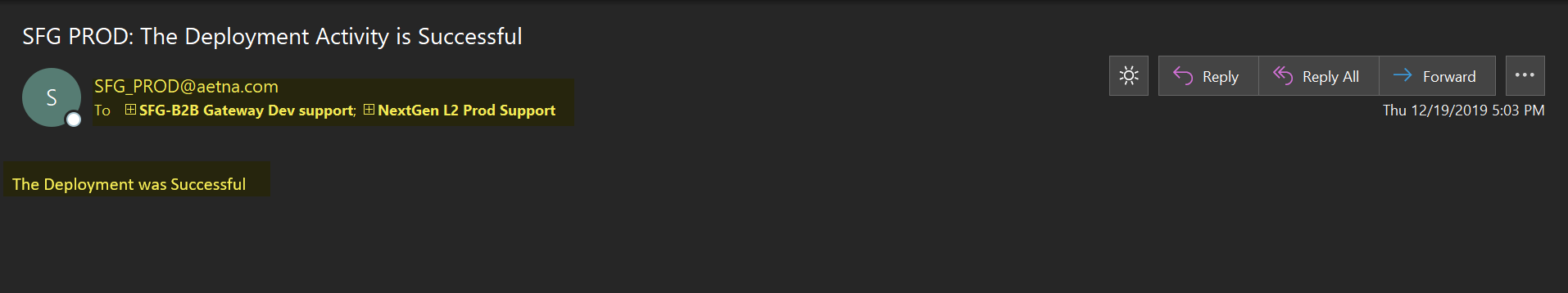


Page 2 of questionnaire; additional details in relation to this deployment; project and product managers, contact information for the gateway teams.

On page 2 of the document provided by Tuberty, there were attachments meant to show the confirmation of a successful deployment from this outlined file transfer. In email attachment [CUEC Number 4-Migration Complete- Know Before You GoB2B Gateway.msg](https://cvshealth.auditboardapp.com/download?file_id=60303), IA observed a communication from team members confirming the success of the migration of files sent to production



In email attachment [CUEC Number 4-SFG PROD The Deployment Activity is Successful.msg](https://cvshealth.auditboardapp.com/download?file_id=60304), IA observed an automated message from the SFG Prod. Aetna email address to the Gateway support email group and production support email group communicating a successful deployment.



Attribute satisfied.

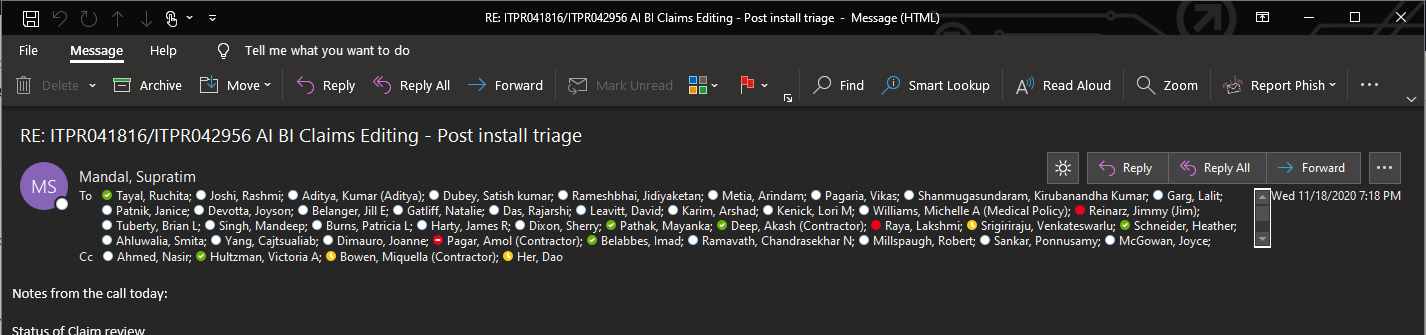
**Sample 13, CUEC #13 (Claims Editing & Prior Authorization)**: User entities are responsible for immediately notifying Novologix of any actual or suspected information security breaches, including compromised user accounts.

IA received artifacts derived out of 1 document request (#5349) from Brian Tuberty, Dir. IT Program Management on 01/28/2021. IA also received additional information via email from Victoria Hultzman, Account Manager for Novologix on 02/03/2021.

On 01/28/2021, IA interviewed Brian Tuberty, Dir. IT Program Management on what entities are notified in an event of a suspected information security breach. Brian stated that Daily triage meetings concerning every aspect of the business, including Novologix, are discussed and acted upon according to the Policies and Procedures provided by the Business (See CIST-0004 – Information Security Policy). IA also observed that Victoria Hultzman, Account Manager for Novologix and Jimmy Reinarz, Executive IT Advisor, Novologix Architecture, are actively involved in the daily triage meetings with Brian, his team, and the business operation unit. Any actual or suspected information breach with regards to Novologix is discussed and addressed respectively. Brian also made it expressly clear that an event such as a security breach is yet to occur within the system; however, training on the proper business procedures to be carried out by team members are available and have been administered (See [CUEC Number 13-Employee Training](https://cvshealth.auditboardapp.com/download?file_id=60301&name=CUEC%20Number%2013-Employee%20Training.docx), referenced on Page 15).

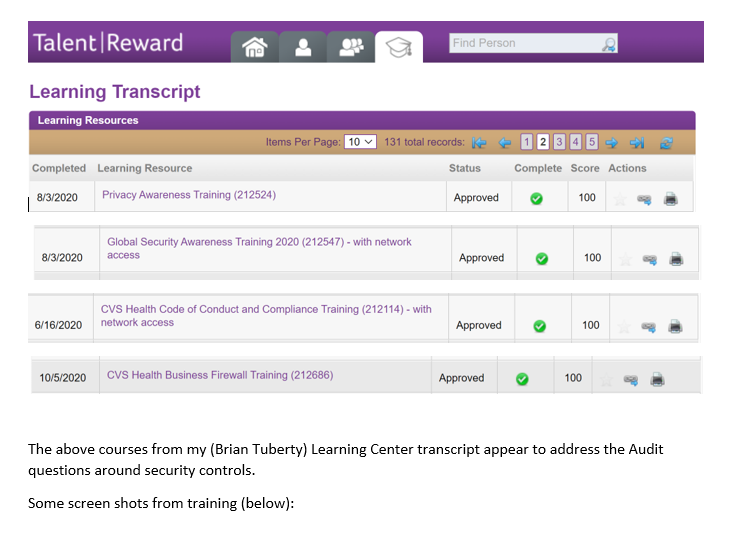
On 02/03/2021, IA received via email from Victoria Hultzman, Account Manager for Novologix, a series of Policy and Procedures governing application security and escalation procedures in an event of a suspected information security breach. Victoria confirmed that Novologix uses the same CVS enterprise policies surrounding security breaches and/or compromised user accounts (See CIST-0004 – Information Security Policy). Victoria also provided documentation on the comprehensive set of application security requirements which outline the procedures required to ensure confidentiality, integrity and availability of confidential information (See [CUEC Number 13-CIST-0056 – Application Security Standard).](https://cvshealth.auditboardapp.com/download?file_id=60295&name=CUEC%20Number%2013-CIST-0056%20-%20Application%20Security%20Standard.pdf) AI observed that when a potential security breach has been identified by Novologix, and further discussed during the Daily triage meetings, the Privacy office gets involved, takes leadership and coordinates every future correspondence relating to the potential security breach with the Business areas, Novologix and every connected entity involved (See [CUEC Number 13-CHIP-0020 – CVS Health Corporate Breach Notification Policy and Procedure](https://cvshealth.auditboardapp.com/download?file_id=60299&name=CUEC%20Number%2013-CHIP-0020%20-%20CVS%20Health%20Corporate%20Breach%20Notification%20Policy%20and%20Procedure.pdf), referenced on Page 16).

**SAMPLE OF PARTICIPANTS INVOLVED IN DAILY TRIAGE MEETING WITH BRIAN AND TEAM**

v

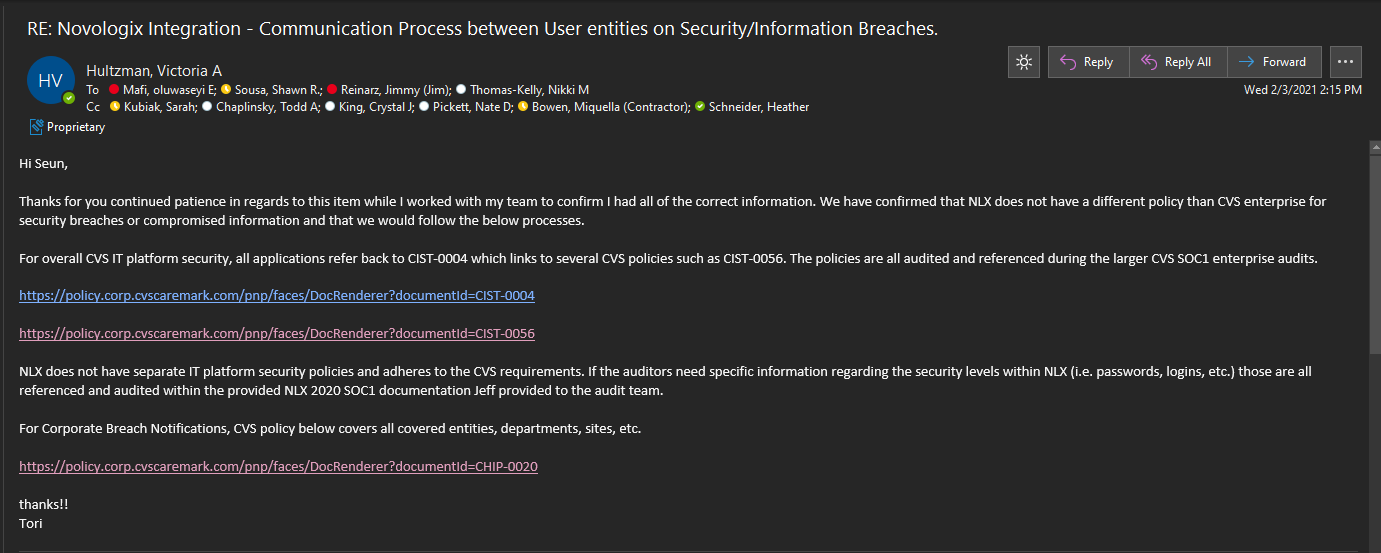
MNMNNB

IA noted in a screenshot provided by Brian Tuberty, Dir. IT Program Management, that Jimmy Reinarz, Executive IT Advisor, Novologix Architecture and Victoria Hultzman, Account Manager for Novologix are active participants in the Daily Triage meetings with Brian’s team and business operations

**EMPLOYEE TRAINING**

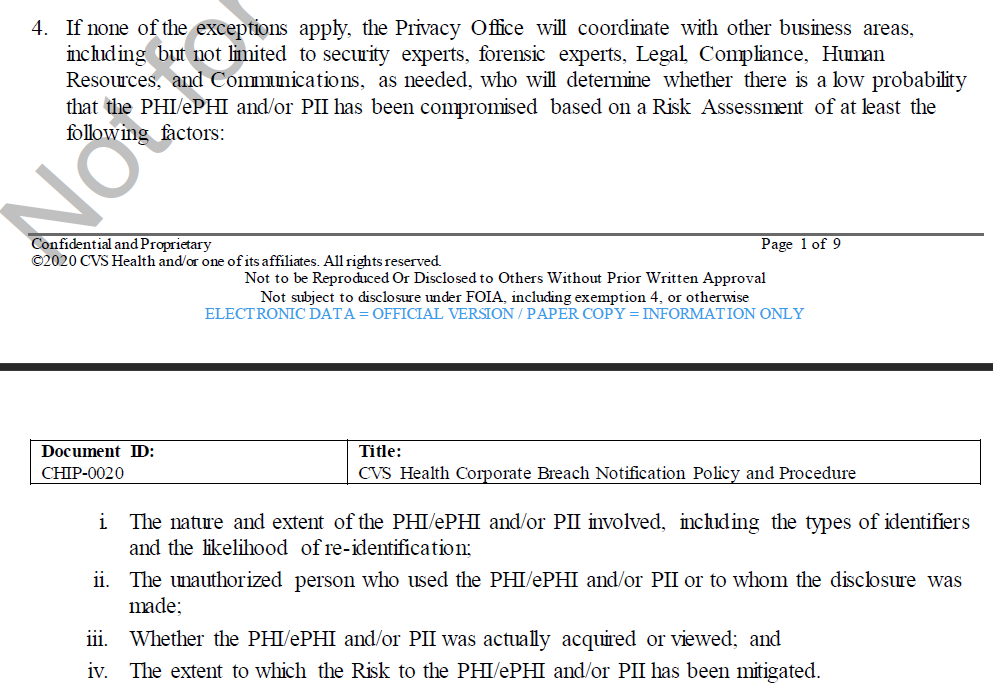
IA noted in a screenshot provided by Brian Tuberty, Dir. IT Program Management, that trainings have been administered to his team members on appropriate protocols surrounding privacy, global security, and CVS code and compliance

**SECURITY AND ESCALATION POLICY AND PROCEDURES**



Victoria Hultzman, Account Manager for Novologix, provides a series of policies and procedures governing application security and escalation protocols adhered to by Novologix in an event of any actual or suspected information security breaches, including compromised user accounts.

**CVS HEALTH CORPORATE BREACH NOTIFICATION POLICY AND PROCEDURE – CHIP-0020**



IA observed that in an event of a security breach, the privacy office is notified by Novologix. The privacy office then takes leadership with coordinating further correspondence relating to the potential security breach with the Business areas, Novologix and every connected entity involved ([CUEC Number 13-CHIP-0020 – CVS Health Corporate Breach Notification Policy and Procedure](https://cvshealth.auditboardapp.com/download?file_id=60299&name=CUEC%20Number%2013-CHIP-0020%20-%20CVS%20Health%20Corporate%20Breach%20Notification%20Policy%20and%20Procedure.pdf))

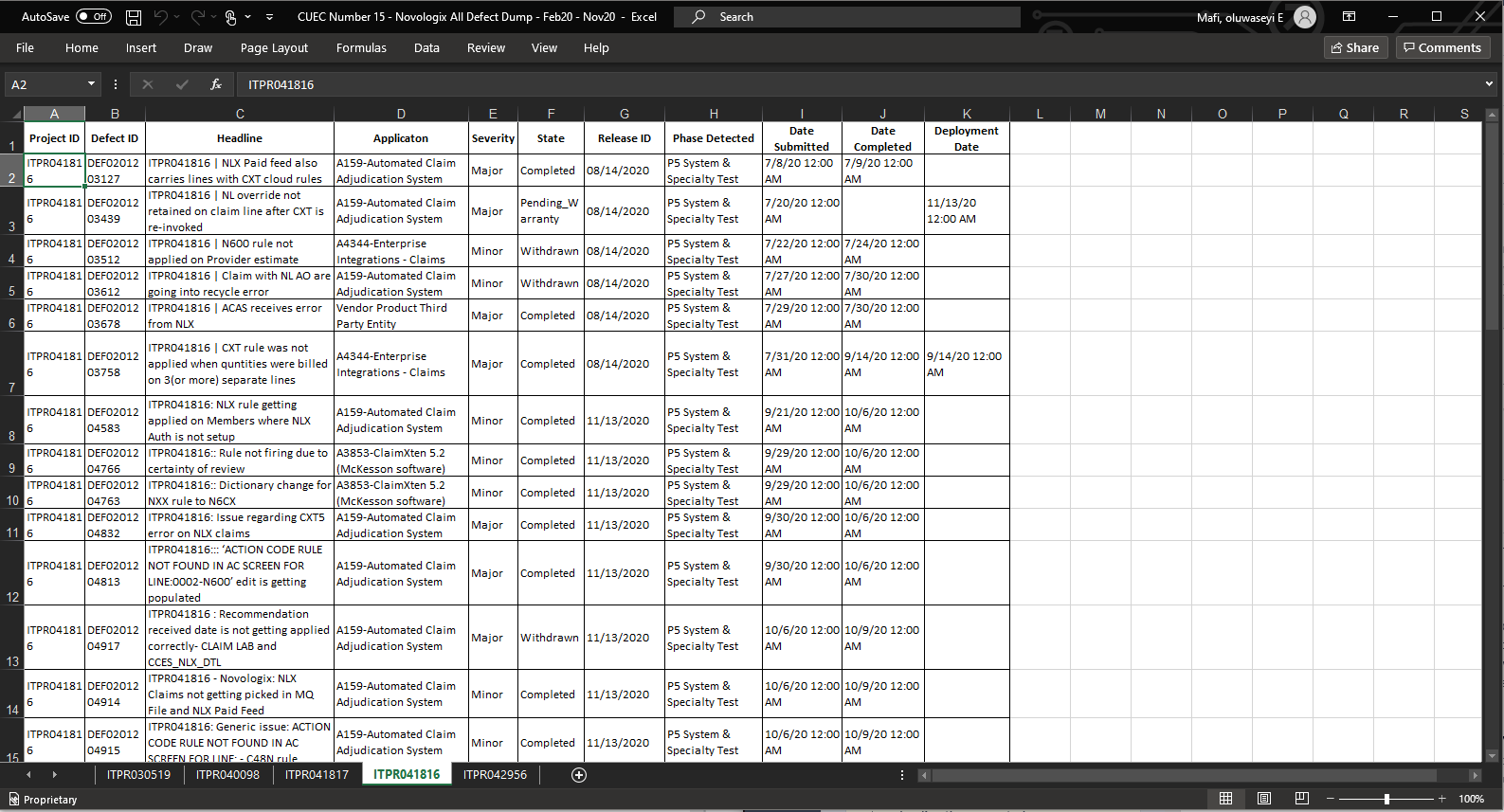
Attribute satisfied.

**Sample 15, CUEC #15 (Claims Editing & Prior Authorization)**: User entities are responsible for communicating any errors or issues that impact their use or ability to process prior authorizations or claims to Novologix on a timely basis. For program changes that do not impact or affect the client; Novologix bares no responsibility.

IA received artifacts derived out of 1 document request (#4168) from Brian Tuberty, Dir. IT Program Management on 01/15/2021.

On 01/15/2021, IA received from Brian Tuberty, Dir. IT Program Management. An excel spreadsheet containing mapping of all Novologix Defect dump from the timeframe of February 20, 2020 to November 20, 2020. (See [CUEC Number 15 – Novologix All Defect Dump file.xlsx](https://cvshealth.auditboardapp.com/download?file_id=58271&name=CUEC%20Number%2015%20-%20Novologix%20All%20Defect%20Dump%20-%20Feb20%20-%20Nov20.xlsx), referenced on page 17). This document lists all the defects by ID number, project date, application affected, severity, state of dump, date submitted and completed, deployment date among other fields.

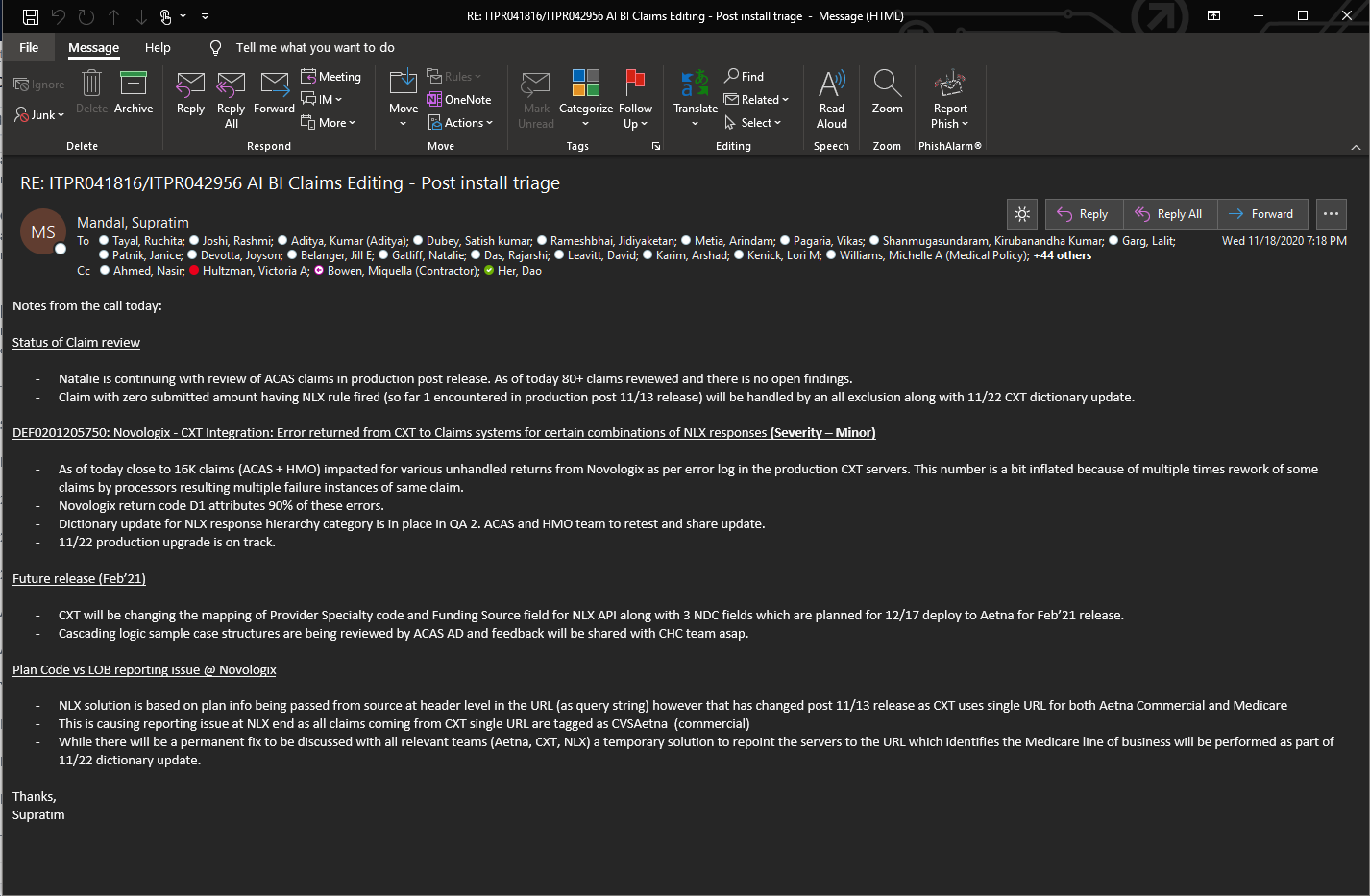
On 01/15/2021, IA also received from Brian Tuberty, , Dir. IT Program Management, a screenshot of an archived email of the post install triage conversation with members of his team discussing status of claims reviewed, error returned, future release plans, and plan code and reporting for Novologix (See [CUEC Number 15 – Post Install Triage – Email Thread.msg](https://cvshealth.auditboardapp.com/download?file_id=58270&name=CUEC%20Number%2015%20-%20Post%20Install%20Traige%20-%20Email%20Thread%20ITPR041816ITPR042956%20AI%20BI%20Claims%20Editing.msg), referenced on page 18). The screenshot referenced a small sample pulled out of the Novologix defect dump file ITPR041816/ITPR042956.

**NOVOLOGIX ALL DEFECT DUMP FILE**

IA noted in the document received from Brain Tuberty that team members have a process in place for communicating any errors and mapping issues to the responsible parties.

Novologix Defect Dump from the timeframe of February 20, 2020 to November 20, 2020.

AI observed the screenshot provided was in reference to a small sample pulled from the Defect Dump File

**AI BI CLAIMS EDITING - POST INSTALL TRIAGE**

IA noted in the screenshot received from Brian Tuberty that team members have a process in place for reviewing issue claims in production post release and outlining each defect per impact severity. AI also observed that the team has a plan mapped out for future releases of provider specialty code and funding source fields, while also including an estimated time of release

IA noted that the responsible parties included in the claims editing post install triage email conversation are user entities responsible for communicating any errors or issues that impact their ability to process claims to Novologix

Attribute satisfied.