Good Morning

Seems there is quite a bit of misunderstanding around this asset. I received a call last week, as did [redacted] inquiring as to why they have not on-boarded with enterprise security services. To understand the findings, one needs to understand the configuration and architecture. Below is the definition from the SSP. The first paragraph is the IOC, which is authorized; and the second is the FOC, which I understand will be funded soon.

Responses to [redacted] questions are included below in red. Also, attached POAM that includes all [redacted] items.

Regards,

[Redacted]
Can you please dig into this and provide me an answer back soonest.

V/r

From: [Redacted]
Sent: Tuesday, July 12, 2016 5:16 PM
To: [Redacted]
Subject: FW: ACES-- security findings and going "live" on

Classification: SECRET//NOFORI

This is an example of one of the systems that I discussed with Martha last week when we talked about how we’re doing assessments and ICD 503 implementation here at NRO. We’ll probably chat about this one again on Thursday.

Can you and your team provide me with nitty gritty details of ACES? I’m assuming it aligns with the “Advanced Collaboration Enterprise Services” system?

- What is the current status of the system?
- What does the heat map assessment look like?
- Is there a tear sheet for the system?
- How in-depth was the assessment? Did they use the RFI methodology to assess?
- How did the documentation (SAR, RAR, etc) look? total findings broken out as;

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Planned Close</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Approved for Release: 2018/07/19 C05112841
I'm not sure who provided Martha with the write-up below, and I'm not sure who provided the "ISSE Comments" (column L) in the attached spreadsheet.

Thanks,

From: [Redacted]
Sent: Tuesday, July 12, 2016 8:05 AM
To: [Redacted]
Subject: FW: ACES-- security findings --SECRET//NOFORN--

Classification: SECRET//NOFORN

 Classified By: [Redacted]
 Derived From: INCG dated 20120213
 Declassify On: 20411232

ACES was only given a ___________________ Given these findings and the fact that they want to connect to ___and____ certain issues need to be addressed and rectified prior to being allowed on either network.

From their documentation:

Therefore, it is imperative that systems be tightened as much as possible to ensure the security of the networks on which they will reside.

Here is a list of the DAO findings that are the most troublesome:
What's a UFC code?
DAO Reps,

The assets listed below have been approved through step 1 in Xacta but do not have a UFC code associated with one or many of the locations. This information is vital. I would appreciate your assistance in encouraging the program to add this information.
ACES Architecture

Overview
A basic ACES system consists of five components:

- **One ACES Server.** The ACES server is the central node in the system. It maps the physical location and dimensions of every screen in the system, and routes commands to and from those screens regarding the information they are displaying.

- **ACES Display Client software.** Every screen in an ACES system, be it a desktop display, a tablet, or a single tile in a video wall, has its own client. (The client is software that runs on the device or on a small computer attached to the screen.) The client's job is to communicate with the ACES Server:
  - The Client tells the Server about the various windows it is currently displaying
  - The ACES Server tells a Client to change what its screen is displaying (eg, "move this window to the left", or "resize this window"). The ACES Server receives these commands from the web server.

- **ACES Desktop Client.** The desktop client performs the same role as the display client: displaying pixels at the request of the ACES Server. However, the desktop client also gives end users the ability to manipulate those pixels through a GUI.

- **ACES Ingest.** This is a special process that runs on ACES Video Ingest Workstations to provide a mechanism for ingesting and manipulating video feeds from various sources. It is a specialized version of the ACES Desktop Client that includes the ability to ingest video feeds from other sources.

- **One ACES Web Server.** The web server gathers information about each Client--its location and the windows it is displaying--from the ACES Server, and (as mentioned above) sends commands to the Clients through the ACES Server. The ACES Web Server is a web based interface provided to manipulate geospatial coordinates of pixel data.

ACES Server
The majority of ACES processing occurs on the ACES Server. The ACES Server runs as a single threaded process on a Linux machine under the name "ACES-server". The ACES Server is coded in Python and runs within a Python 3.x environment. The ACES Server process brokers messages among all ACES Clients. The ACES Server currently subscribes to ports 5566 (receiver) and 5567 (sender). We selected these ports to avoid conflicts with well-established ports such as those described in Service Port and Transport Registry and to avoid known malicious exploit ports described in this intrusion detection FAQ.

ACES Web Server
The ACES Web Server is the primary interface that ACES users use to interact with the system. The ACES Web Server content is also called the ACES Console. It presents a visual map of all of
the pixels registered with the ACES environment along with all of the content mapped to those pixels. The user may add, remove, move and/or resize content via the ACES Web Server. The ACES Web Server runs as a single threaded process on a Linux machine under the name "ACES-webserver". The ACES Web Server is coded in Python and runs within a Python 3.x environment. The ACES Web Server presents information to users via a JavaScript-based web browser application. While configurable, the ACES Web Server currently listens for TCP requests on port 8888. Port 8888 is traditionally used by web servers to serve test pages. ACES Web Server communicates with the ACES Server via ports 5567 (receiver) and port 5566 (sender). We selected these ports to avoid conflicts with well-established ports such as those described in Service Port and Transport Registry and to avoid known malicious exploit ports described in this intrusion detection FAQ.

ACES Desktop Client

The ACES Desktop Client is a process that runs on a user's desktop machine to interact with the ACES environment. The ACES Desktop Client process runs as a single threaded process on a Linux machine under the name "ACES-desktop-client". ACES Desktop Client runs under the Linux KDE Plasma Desktop environment. It is coded in Python and runs within a Python 3.x environment. The ACES Desktop Client communicates with the ACES Server via ports 5567 (receiver) and port 5566 (sender). We selected these ports to avoid conflicts with well-established ports such as those described in Service Port and Transport Registry and to avoid known malicious exploit ports described in this intrusion detection FAQ.

ACES Ingest

The ACES Ingest process runs on specialized ACES Video Ingest Workstations. It allows for the ingest of video feeds from provided thick client desktops or other video sources. ACES Ingest runs under the Linux KDE Plasma Desktop environment. It is coded in Python and runs within a Python 3.x environment. The ACES Ingest communicates with the ACES Server via port 5568 but can be configured to communicate on any port. We selected these ports to avoid conflicts with well-established ports such as those described in Service Port and Transport Registry and to avoid known malicious exploit ports described in this intrusion detection FAQ.

ACES Display Client

The ACES Display Client is a visually interactive component of the ACES environment. Unlike the ACES Desktop Client, the ACES Display Client only presents visual information and is not interactive like a desktop. It functions as a blank canvas that manipulates pixels for displaying ACES content. The ACES Desktop Client process runs as a single threaded process on a Linux machine under the name "ACES-display-client". It is coded in Python and runs within a Python 3.x environment. The ACES Display Client communicates with the ACES Server via ports 5567 (receiver) and port 5566 (sender). We selected these ports to avoid conflicts with well-established ports such as those described in Service Port and Transport Registry and to avoid known malicious exploit ports described in this intrusion detection FAQ.
LOGINS: the default login is ACES/ACES. We have setup the environment so that the default user does not need to login - they are simply presented with a desktop without any login required. They can however lock their screen if they need to get up from their desk.

Privileged users have individual/unique accounts on the photon compute server. In order to login as a privileged user, the user must login to the photon compute server either at console or via ssh from an ACES connected machine (i.e. logins from outside of the ACES network are NOT permitted). The privileged user has a private PKI key that matches a public key on all of the ACES machines. Once a privileged user logs in with their individual login, they can ssh root@<aces_node> to access privileged commands throughout the ACES network.

A functional diagram of the Blackmagic HDMI to SDI converter is below.
Table of Continents

Table of Contents

Table of Continents ................................................................. 2

ACES Architecture ................................................................. 3
  Overview .............................................................................. 3
  ACES Server ....................................................................... 4
  ACES Web Server ............................................................. 4
  ACES Desktop Client .......................................................... 5
  ACES Ingest ....................................................................... 5
  ACES Display Client .......................................................... 5
  Hardware ............................................................................ 6
  Networking ......................................................................... 6
  Separation of Roles ............................................................ 7
  Least Privileged Users ....................................................... 8
  Audit Log .......................................................................... 9
  Password Policy ............................................................... 9
  Account Enforcement ......................................................... 10
  Disabling Unnecessary Services .......................................... 10
  Access Control ................................................................... 11
  Warning Banner ................................................................ 12
  Malicious Code/Antivirus Protection ..................................... 12
  Video Ingest ....................................................................... 12
  ACES JCC ......................................................................... 14

IOCs Functional Capabilities .................................................... 18
  General ACES Capabilities .................................................. 18
  Video Ingest Workstation Capability ..................................... 18
    Explicitly out of scope for IOC .......................................... 19
  IOC equipment list ........................................................... 20
ACES Architecture

Overview

A basic ACES system consists of five components:

- **One ACES Server.** The ACES server is the central node in the system. It maps the physical location and dimensions of every screen in the system, and routes commands to and from those screens regarding the information they are displaying.

- **ACES Display Client** software. Every screen in an ACES system, be it a desktop display, a tablet, or a single tile in a video wall, has its own client. (The client is software that runs on the device or on a small computer attached to the screen.) The client's job is to communicate with the ACES Server:
  - The Client tells the Server about the various windows it is currently displaying
  - The ACES Server tells a Client to change what its screen is displaying (e.g., "move this window to the left", or "resize this window").

- **ACES Desktop Client.** The desktop client performs the same role as the display client: displaying pixels at the request of the ACES Server. However, the desktop client also gives end users the ability to manipulate those pixels through a GUI.

- **ACES Ingest.** This is a special process that runs on ACES Video Ingest Workstations to provide a mechanism for ingesting and manipulating video feeds from various sources. It is a specialized version of the ACES Desktop Client that includes the ability to ingest video feeds from other sources.

- **One ACES Web Server.** The web server gathers information about each Client—its location and the windows it is displaying—from the ACES Server, and (as mentioned above) sends commands to the Clients through the ACES Server. The ACES Web Server is a web based interface provided to manipulate geospatial coordinates of pixel data.
ACES Server

The majority of ACES processing occurs on the ACES Server. The ACES Server runs as a single threaded process on a Linux machine under the name "ACES-server". The ACES Server is coded in Python and runs within a Python 3.x environment. The ACES Server process brokers messages among all ACES Clients. The ACES Server currently subscribes to ports 5566 (receiver) and 5567 (sender). We selected these ports to avoid conflicts with well-established ports such as those described in Service Port and Transport Registry and to avoid known malicious exploit ports described in this intrusion detection FAQ.

ACES Web Server

The ACES Web Server is the primary interface that ACES users use to interact with the system. The ACES Web Server content is also called the ACES Console. It presents a visual map of all of the pixels registered with the ACES environment along with all of the content mapped to those pixels. The user may add, remove, move and/or resize content via the ACES Web Server.

The ACES Web Server runs as a single threaded process on a Linux machine under the name "ACES-webserver". The ACES Web Server is coded in Python and runs within a Python 3.x environment. The ACES Web Server presents information to users via a JavaScript-based web browser application. While configurable, the ACES Web Server currently listens for TCP requests on port 8888. Port 8888 is traditionally used by web servers to serve test pages. ACES Web Server communicates with the ACES Server via ports 5567 (receiver) and port 5566 (sender). We selected these ports to avoid conflicts with well-established ports such as those described in Service Port and Transport Registry and to avoid known malicious exploit ports described in this intrusion detection FAQ.
ACES Desktop Client

The ACES Desktop Client is a process that runs on a user's desktop machine to interact with the ACES environment. The ACES Desktop Client process runs as a single threaded process on a Linux machine under the name "ACES-desktop-client". ACES Desktop Client runs under the Linux KDE Plasma Desktop environment. It is coded in Python and runs within a Python 3.x environment. The ACES Desktop Client communicates with the ACES Server via ports 5567 (receiver) and port 5566 (sender). We selected these ports to avoid conflicts with well-established ports such as those described in Service Port and Transport Registry and to avoid known malicious exploit ports described in this intrusion detection FAQ.

ACES Ingest

The ACES Ingest process runs on specialized ACES Video Ingest Workstations. It allows for the ingest of video feeds from provided thick client desktops or other video sources. ACES Ingest runs under the Linux KDE Plasma Desktop environment. It is coded in Python and runs within a Python 3.x environment. The ACES Ingest communicates with the ACES Server via port 5568 but can be configured to communicate on any port. We selected these ports to avoid conflicts with well-established ports such as those described in Service Port and Transport Registry and to avoid known malicious exploit ports described in this intrusion detection FAQ.
ACES Display Client

The ACES Display Client is a visually interactive component of the ACES environment. Unlike the ACES Desktop Client, the ACES Display Client only presents visual information and is not interactive like a desktop. It functions as a blank canvas that manipulates pixels for displaying ACES content. The ACES Desktop Client process runs as a single threaded process on a Linux machine under the name "ACES-display-client". It is coded in Python and runs within a Python 3.x environment. The ACES Display Client communicates with the ACES Server via ports 5567 (receiver) and port 5566 (sender).

Hardware

Networking
## Separation of Roles

Show different roles are present on the system.

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>At the login screen, login as user &quot;aces&quot; with default password &quot;aces&quot;</td>
<td></td>
</tr>
<tr>
<td>Start a terminal window (Start menu, type Terminal and enter)</td>
<td></td>
</tr>
<tr>
<td><code>ssh &lt;user&gt;@photon.nro.aces-aoe.com</code></td>
<td></td>
</tr>
<tr>
<td><code>ssh -i &lt;private_key_file&gt;</code> <code>root@photon.nro.aces-aoe.com</code></td>
<td></td>
</tr>
<tr>
<td>User enters private key password</td>
<td></td>
</tr>
</tbody>
</table>
Notes:
- Privileged User access is **only** granted on photon.nro.aces-ace.com. In other words, Privileged Users cannot login directly from a workstation.
- This provides us a single point of auditability for all root user access.

**Least Privileged Users**

Show that administrators only have necessary privileges.

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>At the login screen, login as user &quot;aces&quot; with default password &quot;aces&quot;</td>
<td></td>
</tr>
<tr>
<td>Start a terminal window (Start menu, type Terminal and enter)</td>
<td></td>
</tr>
<tr>
<td><code>ls -al /root</code></td>
<td></td>
</tr>
<tr>
<td><code>ssh &lt;user&gt;@photon.nro.aces-ace.com</code></td>
<td></td>
</tr>
<tr>
<td><code>ssh root@ws1.nro.aces-ace.com</code>. Enter the ssh private key password associated with &lt;user&gt;</td>
<td></td>
</tr>
<tr>
<td><code>ls -al /root</code></td>
<td></td>
</tr>
</tbody>
</table>
Audit Log

Show the Audit information generated by the operating system is collected in logs.

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>At the login screen, login as user &quot;aces&quot; with default password &quot;aces&quot;</td>
<td></td>
</tr>
<tr>
<td>Start a terminal window (Start menu, type Terminal and enter)</td>
<td></td>
</tr>
<tr>
<td>Is -al /var/log</td>
<td></td>
</tr>
</tbody>
</table>

Password Policy

Strength of passwords

There is only one non-privileged user in the ACES environment. That user is 'aces' and has a password of 'aces'.
Each privileged user generates a public and private key pair for use within the NRO ACES environment. The public key is placed in the 
/home/aces/.ssh/authorized_keys file and the /root/.ssh/authorized_keys file. When a privileged user attempts to ssh into a Photon Linux machine, the privileged user's private key is compared against the public key in the candidate authorized_keys file. Privileged users on photon have PKI keys installed on every Photon Linux machine in the ACES environment.

**Account Enforcement**

Lock out user after [failed login attempts].

ACES does not implement this policy.

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>NA</td>
<td></td>
</tr>
</tbody>
</table>

**Disabling Unnecessary Services**

Minimizing services operating to those utilized.

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>At the login screen, login as user &quot;aces&quot; with default password &quot;aces&quot;</td>
<td></td>
</tr>
<tr>
<td>Start a terminal window (Start menu, type Terminal and enter)</td>
<td></td>
</tr>
<tr>
<td>systemctl --state=active</td>
<td></td>
</tr>
</tbody>
</table>

Approved for Release: 2018/07/19 C05112841
Notes: ACES only enables necessary services. This test verifies the list of active services.

### Access Control

**Discretionary Access Control**

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>NA</td>
<td></td>
</tr>
</tbody>
</table>

### Patch Verification

Patch level verification for the operating system.

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>At the login screen, login as user “aces” with default password “aces”</td>
<td></td>
</tr>
<tr>
<td>Start a terminal window (Start menu, type Terminal and enter)</td>
<td></td>
</tr>
<tr>
<td><code>dpkg -l</code></td>
<td></td>
</tr>
</tbody>
</table>
Warning Banner

Legal notification banner issued to user prior to system access.

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>NA</td>
<td></td>
</tr>
</tbody>
</table>

Malicious Code/ Antivirus Protection

Virus detection.

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>NA</td>
<td></td>
</tr>
</tbody>
</table>

Video Ingest

Will complete after meeting with COMM & Cross Domain Solution (CDS) team

A functional diagram of the Blackmagic HDMI to SDI converter is below.
IOC Functional Capabilities

This section contains a list of the high-level functional requirements for the initial operating capability (IOC) version of ACES deployed to the JCC Westfields facility.

General ACES Capabilities

Video Ingest Workstation Capability
Explicitly out of scope for IOC

The following items are explicitly out of scope for IOC. This list is not exhaustive. If a capability is not listed above as explicitly supported, then it will NOT be implemented in IOC. This list is here for guidance only.
IOC equipment list

Below is the major hardware components of the initial operating capability for ACES JCC Westfields. Additional peripherals such as

Key items NOT included below that will be provided by NRO:
<table>
<thead>
<tr>
<th>POA&amp;M Nbr</th>
<th>Title</th>
<th>Creation Date</th>
<th>Weaknesses</th>
<th>CAT</th>
<th>POC</th>
<th>Resource Required</th>
<th>Scheduled Completion Date</th>
<th>Comments</th>
<th>ISSU Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>AC-2.3 - Account Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>AC-6 and AC-8.5 - Least Privilege</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>AC-7.a-b, 7.1 - Unsuccessful Login Attempts</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>AU-2.a-d, 2.3, AU-5-3.2, AU-12.a-c, 12.1-c - Audit Events</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>AU-10-10.5 - Non-repudiation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>IA-2.5.a-b - Identification and Authentication</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>AU-8, 8.1 - Time Stamps</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Public Key Enablement (PKE) {IA.6(2,1)}</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>POA&amp;M Nbr</td>
<td>Title</td>
<td>Creation Date</td>
<td>Weaknesses</td>
<td>CAT</td>
<td>POC</td>
<td>Resource Required</td>
<td>Scheduled Completion Date</td>
<td>Comments</td>
<td>SS&amp;I Comments</td>
</tr>
<tr>
<td>-----------</td>
<td>------------------------------------------------------</td>
<td>---------------</td>
<td>------------</td>
<td>-----</td>
<td>-----</td>
<td>-------------------</td>
<td>---------------------------</td>
<td>----------</td>
<td>---------------</td>
</tr>
<tr>
<td>9</td>
<td>Enterprise Audit (AU-6/3)</td>
<td>6/30/2016</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Enterprise Vulnerability Scanning Service (EVSS) (RA-5/19)</td>
<td>6/30/2016</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Vulnerability Assessment / Scans (RA-6.a)</td>
<td>6/30/2016</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>BIOS Security (CM-8.b)</td>
<td>6/30/2016</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Standard Security Banner (AC-8.e.1)</td>
<td>6/30/2016</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Information System Contingency Plan (ISCP) (CP-2.a)</td>
<td>6/30/2016</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Continuous Monitoring Report (CMP) (CA-7)</td>
<td>6/30/2016</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
NLT Thursday, please process a week IATT extension for the ACES program.

Given that out, I don’t have a problem with extending their IATT until we can coordinate a recommendation with OS&CI.

Any issues if I extend the IATT for out this week in I don’t want them to have to turn the system off, and back on again. It is disruptive to their operations.
I agree – any approvals should be clear that the approval is for the currently instantiated version and connectivity only. Any future changes/phases require additional review (and most certainly testing) prior to approval. Like CSCF, let's put a recommendation together and send it to Terry, and Martha for comments before we tweak it and send it forward.

Absolutely! The ATO recommendation is ONLY for WF NROC at this point. They are working towards incorporating the POAM issues for Network Access, and we would address that capability when they can meet the requirements.

Please chime in if you feel that I am misstated anything.

V/r
One thing that stood out on this is their plans for the future. I believe the instance as it is here at WF only and as currently configured is an acceptable risk. As they move forward with their additional plans to add West and potentially engage externally we should have them come back for reassessment and incremental approvals as each is potentially a security relevant change. Is that factored into your recommendation?

Sirs,

Any direction on how we should be proceeding with this? Their IATT expires Friday, the VIAB is done with their analysis of this system, however they are comparing this code to the suspect TDN code of yesteryear. (the coding is in separate languages, so both and I are doubtful that they will draw any similarities between the two.)

- If we withdraw the IATT they will be forced to turn the system back off. (reminder that the system is only at NROC WF today)
- We can extend the IATT. (Much like an ATO since it is being used operationally, it is either on or off to support the NROC mission)
- (my recommendation) We can reinstate the ATO, with their POAM in work, potentially adding the findings that VIAB presented. (This would need to be coordinated behind the scenes through OS&CI Director or Deputy Director)

As I recall from the our discussions with Mr. Duncan, he believed that the (which is what the original ATO covered) That being said, I would like someone above me to make the call, since they made the call to turn it off.

V/r
From: [Redacted]

Sent: Tuesday, September 27, 2016 10:25 AM

Subject: Extension Request for IATT (Operational) for Advanced Collaboration Enterprise Services (ACES)

UNCLASSIFIED

Classification: UNCLASSIFIED

As you know our IATT is set to expire. We have not yet received the final determination from Mr. Duncan on the ATO. I'm requesting a day extension until the VIAB team can give the hot wash brief to Ms. Courtney whom will intern meet with Mr. Duncan.

Regards,

[Redacted]
Dear Sir,

Not sure that would help...let things play out a little more. Only thing I really know is the Ms Courtney (D/OSCI) has a concern, and has not been willing to share what it is outside those not part of CIA...she is questioning us about the testing that was done, when it was her folks that did the testing. My bosses are trying to work this.

Best,

[Signature]

From: [Name]
Sent: Friday, July 15, 2016 9:28 AM
To: [Name]
Subject: RE: ACES--security findings and going "live" on

Classification:SECRET//NOFORN

Classified By: [Name]
Derived From: INCG dated 20120213
Declassify On: 20411231

Copy all...appreciate your support and am standing by (if needed)...

From: [Name]
Sent: Friday, July 15, 2016 9:08 AM
To: [Name]
Subject: RE: ACES--security findings and going "live" on

Classification:SECRET//NOFORN

Classified By: [Name]
Derived From: INCG dated 20120213
Declassify On: 20411231

—from above...

From: [Name]
Sent: Friday, July 15, 2016 8:50 AM
To: [Name]
Subject: RE: ACES--security findings and going "live" on

Classification:SECRET//NOFORN

Classified By: [Name]
Derived From: INCG dated 20120213
Declassify On: 20411231

—from above...
More than happy to set-up a meeting early next week with those who have questions and answer them. I’d like it to be a comprehensive Q&A though...I do not want to have to keep educating people over and over again about ACES like we’ve been doing for over 18 months.

Thank you.

Best,

FYI.
Please take no action, nut be aware someone isn’t a fan...
Heads up. I will be asking for more details on this system.

From: [Redacted]
Sent: Tuesday, July 12, 2016 5:16 PM
To: [Redacted]
Subject: FW: ACES-- security findings and going "live" on

This is an example of one of the systems that I discussed with Martha last week when we talked about how we're doing assessments and ICD 503 implementation here at NRO. We'll probably chat about this one again on Thursday.

Can you and your team provide me with nitty gritty details of ACES? I'm assuming it aligns with the "Advanced Collaboration Enterprise Services" system?

- What is the current status of the system?
- What does the heat map assessment look like?
- Is there a tear sheet for the system?
- How in-depth was the assessment? Did they use the REL methodology to assess?
- How did the documentation (SAR, RAR, etc) look?

I'm not sure who provided Martha with the write-up below, and I'm not sure who provided the "ISSE Comments" (column l) in the attached spreadsheet.

Thanks,
Good Morning

Seems there is quite a bit of misunderstanding around this asset. I received a call last week, as did Sonny, inquiring as to why they have not on-boarded with enterprise security services. To understand the findings, one needs to understand the configuration and architecture. Below is the definition from the SSP. The first paragraph is the IOC, which is authorized; and the second is the FOC, which I understand will be funded soon.
Responses to questions are included below in red. Also, attached POAM that includes all).

Regards,

---

From: 
Sent: Wednesday, July 13, 2016 5:33 PM
To: 
Cc: 
Subject: FW: ACES-- security findings and going "live" on -- SECRET/MODIFIED

Classification: -- SECRET/MODIFIED

Can you please dig into this and provide me an answer back soonest.

V/r

---

From: 
Sent: Tuesday, July 12, 2016 5:16 PM
To: 
Cc: 
Subject: FW: ACES-- security findings and going "live" on -- SECRET/MODIFIED

Classification: -- SECRET/MODIFIED

This is an example of one of the systems that I discussed with Martha last week when we talked about how we're doing assessments and ICD 503 implementation here at NRO. We'll probably chat about this one again on Thursday.
Can you and your team provide me with nitty gritty details of ACES?

- What is the current status of the system?
- What does the heat map assessment look like?
- Is there a tear sheet for the system?
- How in-depth was the assessment? Did they use the RFI methodology to assess?
- How did the documentation (SAR, RAR, etc) look?

I’m not sure who provided Martha with the write-up below, and I’m not sure who provided the “ISSE Comments” (column L) in the attached spreadsheet.

Thanks,

From: Courtney Martha K NRO USA GOV
Sent: Tuesday, July 12, 2016 8:05 AM
To: 
Subject: FW: ACES-- security findings ---SECRET//NOPORN---

Classification: ---SECRET//NOPORN---

Classified By: _________
Derived From: INCG dated 20120213
Declassify On: 20411231

ACES was only given a _____________________________ Given these findings and the fact that they want to connect to _____________________________ certain issues need to be addressed and rectified prior to being allowed on either network.

From their documentation:
To:  
Cc:  
Date: 14- July 2016  
Subject: Advanced Collaboration Enterprise Services (ACES)

System Boundary: Initial Operation Capability (IOC) - Authorized

(U//FOUO) ACES consists primarily of a server and video switcher that allows analysts the ability to change the presentation view by manipulating pixel space on a monitor from multiple display sources from ___________. ACES eliminates the need for multiple monitors to view multiple screens of data. The display sources are generated from ___________.

System Boundary: Future Operation Capability (FOC) Not Authorized initially includes:

(U//FOUO) ACES installation does require ___________. All of the ACES systems are self-contained on the ACES subnet.

Risk Analysis:

(U//FOUO) In June 2016, a Risk Assessment was performed to evaluate the security controls of the asset as High, Low, Low impact levels for Confidentiality, Integrity and Availability respectively. Analysis of the Risk Assessment Report and negotiations with the program resulted in ___________ as follows.

DAO Rep Recommendation:

(U//FOUO) Based on the agreed upon lien closure dates, recommend a ___ year ATO with POAM for ACES. During this ___ year period, the program needs to pursue an IATT to connect to ___ to obtain enterprise security services to close many of the identified security weaknesses. Additionally, the program needs to begin immediately executing the Continuous Monitoring Plan to keep apprised, manage, and report the asset’s security controls proactively.
Hello Sir-

Please note the Risk Assessment task was just approved by me, moving the asset to Program Acknowledgement. Also, given the visibility of this asset, I completed and loaded the attached RAR into Xacta.

Thanks.

All,

Based on the Program's agreed upon POA&M, I grant the ACES system (asset [redacted]), a [redacted] year ATO w/POA&M. This approval granted today,

Working this approval in email (outside of Xacta) has been pre-coordinated with the SCA, DCA, DAO Rep, and DAO [redacted] (who is on vacation). It is still a requirement for this approval to be completed in Xacta.

Any questions, please contact me at [redacted].
For your action. I'll get the findings from VIAB.

V/r

---

OK, I'll incorporate the latest findings from VIAB into the recommendation and pass through you both before sending it up.

V/r
From: [Redacted]
Sent: Friday, September 23, 2016 1:39 PM
To: [Redacted]
Cc: [Redacted]
Subject: FW: 21-SEPT-2016 SETR on the ACES assessment
Attachments: Sept-21-2016-SETR.docx

Classification: SECRET//TK//REL TO USA, FVEY

Classified By: [Redacted]
Derived From: INCG dated 20120213
Declassify On: 25X1, 20661231

Gentlemen,

We completed the SED SETR this week...assessment from below...great news as we work toward "normalizing" this capability over the longer-term...as we deploy this needed capability across in the short-term.

Next Step: MAEC

Best,
Subject: 21-SEPT-2016 SETR on the ACES assessment --SECRET//TK//REL TO USA, FVEY--

Classification: SECRET//TK//REL TO USA, FVEY

Please post the attached notes and the briefings to the NRO SETR web site for leaders and attendees to access.

SUBJ: (U) Major discussion points/notes from 21-SEPT-2016 SETR.

Topic #1: (U) process triage assessment/recommendations for; “Mission Opportunity 2016-003: Advanced Collaboration Enterprise Services” ACES)

(U) SUMMARY/OVERVIEW Topic -1:

(U) Comments/Discussion:
Request your earliest opportunity to meet with [Name] to discuss ACES [Reference] referenced below. Hopefully during this meeting we will concur on a finalized network diagram including detailed connections and an equipment list. We are hoping to reach a decision on any cross domain issues that stem from ongoing concerns raised by multiple stakeholders.

Thank you,

From:
Sent: Friday, December 18, 2015 12:09 PM
To: 
Cc: 
Subject: FW: IMPORTANT: ACES - SRT - Next Step --- UNCLASSIFIED

Classification: UNCLASSIFIED

Thanks for the discussion today...here's what we agreed to do...

1) Schedule a meeting ASAP with DAO, [ACES Engineer(s)] and diagram the exact ACES capability (server room, being deployed O/A 29 Jan 16. Someone from DAO will do the actual diagramming so that it is done in a way that makes sense to all internal NRO stakeholders. ACES Engineers will be there to support. [Name] will be there to ask questions/receive answers.

2) Once diagramming is complete, DAO (or whomever you designate) will convert it into an appropriate format (e.g., visio, photo, etc.)
Please provide me a couple of dates over the next two weeks that work for DAO/ so that I can coordinate that with the ACES team and get it on the calendar. Let’s be sure to invite from MOD and anyone else that would benefit from attending (e.g., etc.).

Please communicate directly with and in all communications as I will be out of the office beginning 23 Dec.

Best,

=================================================================
Classification: UNCLASSIFIED
=================================================================

Classification: UNCLASSIFIED
From: [Redacted]
Sent: Thursday, December 17. 2015 1:48 PM
To: [Redacted]
Cc: [Redacted]
Subject: FW: IMPORTANT: Xacta Project ACES (Advanced Collaboration Enterprise Services) Installation — UNCLASSIFIED

Classification: UNCLASSIFIED

You were left off the attached. [Redacted] is really pushing an ACES (Advanced Collaboration Enterprise Services). [Redacted] Director Sapp'. I would recommend a meeting with [Redacted] DAO (?), and [Redacted] prior to a meeting with [Redacted] so you can ensure everyone is on the same page.

For the meeting [Redacted] is calling for below, I think it's reached a point that you need to bring the big guns [Redacted] or [Redacted] into the picture!!!

From: [Redacted]
Sent: Thursday, December 17. 2015 11:17 AM

Subject: RE: IMPORTANT: ACES Installation --- UNCLASSIFIED

Classification: UNCLASSIFIED

Hi [Redacted]...just following up... Can we meet tomorrow (before 1500)? Or, worst case next Monday or Tuesday morning?

I need to give the requisite ACES team members a heads up too (that will need to be at the meeting).

Thank you.

Best,
Subject: IMPORTANT: ACES Installation --- UNCLASSIFIED

Classification: UNCLASSIFIED

Hi [Name],

Thank you for your time and assistance on the ACES installation. Director Sapp's Operations is moving through the NRO SRT process with a projected installation approval in O/A 29 Jan 15.

Between now and then, we need to prepare for the install which will be completed by and the ACES Team. Here are key details regarding ACES install:

I'd like to get the ACES Team and team together ASAP to discuss this. Can we meet this week or on Monday or Tuesday (at the very latest) of next week?

Thank you.

Best,
I appreciate you flagging this for our attention. In addition to DD/MS&O's note to you today, I wanted to let you know we are looking at this and will work to improve schedule on this high priority system.

What I found was the project initiated in roughly July with discussions of the basic needs. There were some problems noted early on to include Security approval for the displays. Nonetheless, we provided a ROM on 17 September and funding was eventually received on 13 November.

I will be tdy much of next week so either ________ or myself will get back to you or ________ on schedule.

V/R,

I need your help with an install project in the NROC. We have requested a set of fitment changes to the NROC collaboration spaces and our (called ACES) we are scheduled to install in late January. Our project POC, ________ has
been in routine communication with your team concerning timelines but the current facility schedule dates (below) do not match up with our planned technology install plan. ACES is a high priority project for us and the timelines required extensive coordination with internal & external partners including the Headquarters Air Staff / A2 who is lead for ACES. I know your teams are extremely busy with a multitude of projects across Westfield, but I would appreciate any assistance you can provide to increase priority of this project since it has direct impact to our joint collaboration mission in MOD.

If you need any further detail or have questions, please contact me or __________ Thank you for your consideration.

v/r,

========================================
Classification: UNCLASSIFIED

========================================
Classification: UNCLASSIFIED

========================================
Classification: UNCLASSIFIED

========================================
Classification: UNCLASSIFIED
I would like to brief you on the latest advanced effort coming out of NROC [MOD] called ACES **Advanced Collaboration Enterprise Services (ACES)**.

1. This MOD asset is new and non-operational. Xacta Project: 
2. They gave the 1st initial brief to most of the stakeholders at the MOD ERB on 9 Sept. and I attended.
3. Description:
   a. **(U/FOUO)** ACES consists primarily of a server and video switcher that allows analysts the ability to change the presentation view by manipulating pixel space on the monitor. ACES eliminates the need for multiple monitors to view multiple screens of data. MOD's ACES installation requires
4. RMF Steps 1 & 2 have been closed in Xacta.
5. An IATT Approval Task is currently sitting in the SCAs queue for 1/5.
6. **(U/FOUO)** There is an ACES Demo scheduled for 5 Oct 2015 from 12-1400 at 1401 Wilson Blvd, Level B, Arlington, VA
7. has asked to facilitate a pre-brief prior to demo to respond to any questions we may have.

So I'm just letting you know that will have representation from some of the DCAs. and I will both be there. I have forwarded you the calendar invite. See additional comments below.

Please feel free to contact either or me if you have any additional questions or concerns.

VR,
I am going into surgery on Wednesday and will be out several weeks. This demo cannot wait for me...so, please coordinate and send me an email at ________ or call me at ________ this week with the date/time so I can make it happen.

From:  
Sent: Monday, September 28, 2015 9:13 AM

Subject: RE: ACES Demo and Intro --- UNCLASSIFIED//FOUO

Classification: UNCLASSIFIED//FOUO

Hi [Name],

I think it would be helpful if the ISSM [Name] for ACES also was there to help facilitate the discussion and answer any upfront questions prior to the demo.

Can you please get with [Name] this week with the date/time so I can make it happen.

Thank you!

Best,

---

From:  
Sent: Friday, September 25, 2015 9:43 AM

Subject: RE: ACES Demo and Intro --- UNCLASSIFIED//FOUO

Classification: UNCLASSIFIED//FOUO

Hi [Name],

Can you please give [Name] and myself an overview of your visit and what to expect with the ACES Demo and Intro? Thanks.

---
Hi

I am also Ccing ______ (DAO Rep)...

Hopefully ______ gave you a summary of his visit to the ACES Lab in Arlington last week. ______ and we definitely want all relevant stakeholders to be ACES “smart” as we maneuver through the NRO SRT process to get it accredited and authorized.

We are holding another ACES demo for other NRO leadership on Monday, 5 Oct, from 1200-1400.

It would be great if you can attend...you are cordially invited! ______ you are reinvited as well as your leadership...the DAO).

Please let me know this week if you can make this demo. Thank you.

Best,

From:  
Sent: Monday, September 28, 2015 12:14 PM

Subject: IMPORTANT: ACES Update — UNCLASSIFIED

Classification: UNCLASSIFIED

-----------------------------------------------

Advanced Collaboration Enterprise Services (ACES)
Creating a Common Operating Environment (COE)

This is a bi-weekly status update on ACES for all relevant stakeholders. Highlights/Changes in Red
Best,

Classification: UNCLASSIFIED

Classification: UNCLASSIFIED

Classification: UNCLASSIFIED
From: j
Sent: Thursday, January 14, 2016 1:48 PM
To: 

Subject: IMPORTANT: ACES Update — UNCLASSIFIED

Classification: UNCLASSIFIED

Advanced Collaboration Enterprise Services (ACES)

Creating a Common Operating Environment (COE) for MOD Collaboration Enterprise

This is a weekly status update on ACES for all relevant stakeholders. Highlights/Changes in Red.
Best,

=================================
Classification: UNCLASSIFIED

=================================
Classification: UNCLASSIFIED
From: 
Sent: Tuesday, December 15, 2015 12:12 PM
To: 
Subject: IMPORTANT: ACES Update --- UNCLASSIFIED

Classification: UNCLASSIFIED

Advanced Collaboration Enterprise Services (ACES)

Creating a Common Operating Environment (COE) for MOD Collaboration Enterprise

This is a bi-weekly status update on ACES for all relevant stakeholders. Highlights/Changes in Red.
Best,

Classification: UNCLASSIFIED
Subject: IMPORTANT: ACES Update — UNCLASSIFIED

Classification: UNCLASSIFIED

Advanced Collaboration Enterprise Services (ACES)

Creating a Common Operating Environment (COE)

This is a bi-weekly status update on ACES for all relevant stakeholders. Highlights/Changes in Red.
Best,

Classification: UNCLASSIFIED

Classification: UNCLASSIFIED

Classification: UNCLASSIFIED
Advanced Collaboration Enterprise Services (ACES)

Creating a Common Operating Environment (COE)

This is a bi-weekly status update on ACES for all relevant stakeholders. Highlights/Changes in Red.
Best,

=================================================================================================================================
Classification: UNCLASSIFIED

=================================================================================================================================
Classification: UNCLASSIFIED
Subject: IMPORTANT: ACES Update — UNCLASSIFIED

Classification: UNCLASSIFIED

Advanced Collaboration Enterprise Services (ACES)

Creating a Common Operating Environment (COE) for MOD Collaboration Enterprise

This is a weekly status update on ACES for all relevant stakeholders. Highlights/Changes in Red.
Best,

======================================================================

Classification: UNCLASSIFIED
To:

Subject: IMPORTANT: Weekly ACES Program Update--- UNCLASSIFIED --- UNCLASSIFIED

Classification: UNCLASSIFIED

Advanced Collaboration Enterprise Services (ACES)

Creating a Common Operating Environment (COE) for NRO enterprise operations

This is a weekly status update on ACES for all relevant stakeholders. Highlights/Changes in Red.
Best,

Classification: UNCLASSIFIED
Subject: IMPORTANT: Weekly ACES Update — UNCLASSIFIED

Classification: UNCLASSIFIED

===========================================;==========

Advanced Collaboration Enterprise Services (ACES)

Creating a Common Operating Environment (COE) for MOD Collaboration Enterprise

This is a weekly status update on ACES for all relevant stakeholders. Highlights/Changes in Red.
Subject: IMPORTANT: Weekly ACES Update — UNCLASSIFIED

Advanced Collaboration Enterprise Services (ACES)

Creating a Common Operating Environment (COE) for MOD Collaboration Enterprise

This is a weekly status update on ACES for all relevant stakeholders. Highlights/Changes in Red.
To: 

Subject: IMPORTANT: Weekly ACES Update — UNCLASSIFIED

Classification: UNCLASSIFIED

----------------------------------------

Advanced Collaboration Enterprise Services (ACES)

Creating a Common Operating Environment (COE) for MOD Collaboration Enterprise

This is a weekly status update on ACES for all relevant stakeholders. Highlights/Changes in Red.
Classification: UNCLASSIFIED

Advanced Collaboration Enterprise Services (ACES)

Creating a Common Operating Environment (COE) for MOD Collaboration Enterprise

This is a weekly status update on ACES for all relevant stakeholders. Highlights/Changes in Red.
From:
Sent: Friday, May 20, 2016 11:43 AM
To:

Subject: IMPORTANT: Weekly ACES Update — UNCLASSIFIED.

Classification: UNCLASSIFIED

============================================
Advanced Collaboration Enterprise Services (ACES)

Creating a Common Operating Environment (COE) for MOD Collaboration Enterprise

This is a weekly status update on ACES for all relevant stakeholders. Highlights/Changes in Red.
From: Monaav Mav
Sent: Monday, May 02, 2016 1:40 PM
To: 

Subject: IMPORTANT: Weekly ACES Update — UNCLASSIFIED

Classification: UNCLASSIFIED

Advanced Collaboration Enterprise Services (ACES)
Creating a Common Operating Environment (COE) for MOD Collaboration Enterprise

This is a weekly status update on ACES for all relevant stakeholders. Highlights/Changes in Red.
Subject: IMPORTANT: weekly ACES Update — UNCLASSIFIED

Classification: UNCLASSIFIED

Advanced Collaboration Enterprise Services (ACES)

Creating a Common Operating Environment (COE) for MOD Collaboration Enterprise
This is a weekly status update on ACES for all relevant stakeholders. Highlights/Changes in Red.
Subject: IMPORTANT: Weekly ACES Update — UNCLASSIFIED

Classification: UNCLASSIFIED

Advanced Collaboration Enterprise Services (ACES)

Creating a Common Operating Environment (COE) for MOD Collaboration Enterprise

This is a weekly status update on ACES for all relevant stakeholders. Highlights/Changes in Red.
Advanced Collaboration Enterprise Services (ACES)

Creating a Common Operating Environment (COE) for MOD Collaboration Enterprise

This is a weekly status update on ACES for all relevant stakeholders. Highlights/Changes in Red.
Subject: IMPORTANT: Weekly ACES Update — UNCLASSIFIED

Classification: UNCLASSIFIED

Advanced Collaboration Enterprise Services (ACES)

Creating a Common Operating Environment (COE) for MOD Collaboration Enterprise

This is a weekly status update on ACES for all relevant stakeholders. Highlights/Changes in Red.
Advanced Collaboration Enterprise Services (ACES)

Creating a Common Operating Environment (COE) for MOD Collaboration Enterprise

This is a weekly status update on ACES for all relevant stakeholders. Highlights/Changes in Red.