Office Instruction: CSO-TEMP-2017
Office Instruction Title: Formal Deviation Request Memo
Revision Number: 2.2
Effective Date: November 12, 2015
Primary Contacts: Kathy Lyons-Burke, SITSO
Responsible Organization: OCIO/ISD/PCT
Summary of Changes: CSO-TEMP-2017, “Formal Deviation Request Memo” provides the template that must be used to request a formal deviation or waiver from required cybersecurity requirements for an information system.
Training: As required
ADAMS Accession No.: ML15308A590

<table>
<thead>
<tr>
<th>Concurrency Conducted via email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attendees:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Concurrences</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Primary Office Owner</strong></td>
</tr>
<tr>
<td><strong>Responsible SITSO</strong></td>
</tr>
<tr>
<td><strong>Directors</strong></td>
</tr>
<tr>
<td><strong>Other Stakeholders</strong></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Date of Concurrence</th>
</tr>
</thead>
<tbody>
<tr>
<td>12-Nov-15</td>
</tr>
</tbody>
</table>
Computer Security Template
CSO-TEMP-2017

Formal Deviation Request Memo

1 PURPOSE

CSO-TEMP-2017, “Formal Deviation Request Memo” provides the memorandum template that must be used to request a formal deviation from NRC required security controls. CSO-TEMP-2018, “Deviation Request Memo Enclosure” accompanies the formal memorandum and provides supporting details relevant to the request. This template should be filled out in accordance with CSO-PROS-1324, “System Deviation Request Process.”

This front matter and all explanatory information up through the change history table apply to the template only. The front matter and explanatory information must be removed before completing and submitting the memorandum.

2 TEMPLATE INSTRUCTIONS

The template sections are completed by the system owner’s organization. Information in <blue> in the template should be replaced with the required information and the font color returned to black before submitting the memorandum.

The sensitivity markings in the template are only in effect when the template is populated with system information.

The date of the memorandum is provided where <Memo Date> is shown and formatted as “Month Day, Year.”

The system owner’s first name, middle initial, and last name are provided where <System Owner First_Name X. Last_Name> is shown.

The system owner’s office, region, or Office of Information Services division name is provided where <Office or Region Name> is shown.

The name of the system is provided where <System Name> is shown.

The system acronym is placed wherever <System Acronym> occurs.

The Agencywide Document and Management System (ADAMS) accession number for the referenced document is provided where <Accession Number> occurs.

The primary information system security officer’s (ISSO’s) first name, middle initial, and last name are provided where <Primary ISSO First_Name X. Last_Name> is shown.

The primary system ISSO’s office telephone number is provided where <XXX-XXX-XXXX> is shown.
The alternate ISSO’s first name, middle initial, and last name are provided where <Alternate ISSO First_Name X. Last_Name> is shown.
## CSO-TEMP-2017 Change History

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Description of Changes</th>
<th>Method Used to Announce &amp; Distribute</th>
<th>Training</th>
</tr>
</thead>
<tbody>
<tr>
<td>04-Nov-15</td>
<td>2.2</td>
<td>Administrative change to reflect change in DAA appointment</td>
<td>Posting to OCIO/ISD web page and notification to ISSOs.</td>
<td>Upon request</td>
</tr>
<tr>
<td>29-Apr-14</td>
<td>2.1</td>
<td>Editorial update to fix changing personnel and references</td>
<td>Posting to CSO web page and notification to ISSO forum.</td>
<td>As needed</td>
</tr>
<tr>
<td>19-Mar-12</td>
<td>2.0</td>
<td>Updated memo in accordance with new deviation request process</td>
<td>Distribution by posting on CSO web page</td>
<td>As needed</td>
</tr>
<tr>
<td>13-Jul-10</td>
<td>1.1</td>
<td>Reformatted to NRC template</td>
<td>Distribution by posting on CSO web page</td>
<td>As needed</td>
</tr>
<tr>
<td>09-Jul-10</td>
<td>1.0</td>
<td>Updated DAA names / titles</td>
<td>Distribution by posting on CSO web page</td>
<td>As needed</td>
</tr>
</tbody>
</table>
Attachment

Formal Deviation Request Memo Template
<Memo Date>

MEMORANDUM TO: Darren B. Ash  
Chief Information Officer  
Glenn M. Tracy  
Deputy Executive Director for Materials, Waste, Research, State, Tribal, Compliance, Administration, and Human Capital  
Office of the Executive Director for Operations  
Michael R. Johnson  
Deputy Executive Director for Reactor and Preparedness Programs  
Office of the Executive Director for Operations  

FROM: <System Owner Firstname X. Lastname>, Director  
<Office or Region Name>  
SUBJECT: FORMAL DEVIATION REQUEST FOR THE <SYSTEM NAME>  

This memo constitutes my formal request for a deviation from specific cybersecurity requirements for the <System Name> (<System Acronym>). The <System Acronym> system is not able to fully comply with all current cybersecurity requirements due to current limitations.  

Enclosure:  
As stated  

CONTACT: <Primary ISSO First_Name X. Last_Name> <Office or Region Name>  
Telephone number (<XXX-XXX-XXXX>)  

cc: <Primary ISSO First_Name X. Last_Name>, Primary ISSO  
<Alternate ISSO First_Name X. Last_Name>, Alternate ISSO  
T. Rich, OCIO/ISD  
K. Lyons-Burke, OCIO/ISD  
T. Graham, OCIO/ISD  
G. Somerville, OCIO/ISD
The enclosed Deviation Request Details Spreadsheet (<Accession Number>) identifies the details associated with each deviation.

- the cybersecurity requirement that cannot be met;
- the source that identified non-compliance with the cybersecurity requirement;
- any associated POA&M items;
- details of the requested deviation;
- the reason why the requirement cannot be met, including the resource implications and associated evidence;
- the risk level of the weakness as determined by the original source;
- the compensating controls and mitigating factors that partially or fully mitigate the risk; and
- the residual cybersecurity risk after factoring in the compensating controls and mitigating factors.