Standard ID.GV: Authorizing Officials

February 11, 2021

U.S. Department of Education (ED)
Office of the Chief Information Officer (OCIO)
Information Assurance Services (IAS)

Questions about the policies outlined in this document should be directed to Information Assurance Services (IAS) at OCIO_IAS@ed.gov
APPROVAL

Steven Hernandez
Digitally signed by Steven Hernandez
Date: 2021.02.11 12:38:45 -05'00'

Steven Hernandez
Director, IAS/Chief Information Security Officer (CISO)
Revision History

The table below identifies all changes that have been incorporated into this document.

<table>
<thead>
<tr>
<th>Version</th>
<th>Draft Date</th>
<th>Summary of Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>10/21/2019</td>
<td>Initial draft with updated comments</td>
</tr>
<tr>
<td>0.2</td>
<td>4/1/2020</td>
<td>Revised per CISO review and comment</td>
</tr>
<tr>
<td>0.3</td>
<td>6/10/2020</td>
<td>Addition of Risk Acceptance Form (RAF) guidelines</td>
</tr>
<tr>
<td>1.0</td>
<td>6/17/2020</td>
<td>Final review for format and syntax</td>
</tr>
<tr>
<td>1.1</td>
<td>6/22/2020</td>
<td>Addition of Exception Policy</td>
</tr>
<tr>
<td>1.2</td>
<td>1/13/2021</td>
<td>Reviewed for accuracy and timeliness. Updated Risk acceptance and policy exception</td>
</tr>
</tbody>
</table>
Table of Contents

1 INTRODUCTION ............................................................................................................. 1

1.1 Purpose..................................................................................................................... 1

1.2 Scope....................................................................................................................... 1

2 SYSTEM SECURITY PLAN REVIEW AND ACCEPTANCE PROCESS FOR HVAs, HIGH, MODERATE AND LOW IMPACT SYSTEMS ...................................................... 1

2.1 SSP Review Checklist.............................................................................................. 2

2.2 SSP Review and Acceptance Process ........................................................................ 2

3 ATO PACKAGE REVIEW AND ACCEPTANCE PROCESS............................................ 2

3.1 ATO Package Review Post Assessment Phase ........................................................... 2

3.2 ATO Package Review and Acceptance Process ......................................................... 2

4 DELEGATION OF AO RESPONSIBILITIES FOR LOW IMPACT SYSTEMS .......... 2

5 APPOINT OR REPLACE THE ISO FOR ALL SYSTEMS UNDER AO AUTHORITY .... 3

6 AO Approval of Accepted Risk.................................................................................... 3

7 RISK ACCEPTANCE/POLICY EXCEPTIONS ................................................................. 3

8 APPENDIX A: ACRONYMS............................................................................................ 4
1 INTRODUCTION
Under the authority of the Department of Education (ED) Chief Information Officer (CIO), the
Chief Information Security Officer (CISO) bears the primary responsibility to ensure compliance to
the Federal Information Security Modernization Act (FISMA); the National Institute of Standards
and Technology (NIST); the Office of Management and Budget (OMB); and all applicable laws,
directives, policies, and directed actions on a continuing basis.

In keeping with this responsibility, this document establishes the compliance standards for the
following:

- Conducting security reviews for System Security Plans (SSP) and associated artifacts
- Conducting security reviews for Authority to Operate (ATO) packages
- Delegation of Authorizing Official (AO) authorities for low-impact systems
- Appointing or replacing the respective Information System Owner (ISO) for the systems
  under the AO authority
- The approval steps and process for the AO Approval of Accepted Risk

1.1 Purpose
This document establishes Departmental compliance standards for the SSP security review process
for High Value Assets (HVAs); High, Moderate, and Low-impact systems; the ATO security
authorization process; delegation of AO authorities for the low impact systems; the appointment of
ISO for those systems under AO authority and the AO Approval of Accepted Risk process. This
document supersedes any prior documentation establishing such standards.

1.2 Scope
The standards established in this document apply to all employees, contractors, and users
authorized to access ED information systems. The scope of this document covers the standards
required for the review and approval of SSP and ATO for HVAs, high, moderate, and low impact
systems; the delegation of AO authorities for low-impact systems (OIG systems are excluded from
this standard); the rules for ISO appointment for systems under the AO authority and the AO
Approval of Accepted Risk process.

2 SYSTEM SECURITY PLAN REVIEW AND ACCEPTANCE PROCESS
FOR HVAs, HIGH, MODERATE AND LOW IMPACT SYSTEMS
All federal systems have some level of sensitivity and require protection and detailed review as part
of meeting the requirements of the FISMA. As such, each SSP must provide detailed
documentation for the protection of a system. The SSP Review and Acceptance Process will
provide a documented and repeatable method of providing system security reviews. This process
will enforce a review of the critical elements as documented in the below SSP review checklist
required for each respective system, based on the latest mandates.
2.1 SSP Review Checklist
The SSP review checklist of AO acceptance criteria can be found in the AO Standard Operating Procedures (SOP).

2.2 SSP Review and Acceptance Process
The SSP Review and Acceptance Process is a formal process which references security requirements for an information system and ensures security controls are in place or planned for meeting those requirements as outlined in the NIST SP 800-18. According to the NIST 800-171, the SSP should be used to describe enduring exceptions to the security requirements. Any individual, isolated, or temporary deficiencies should be managed through Plans of Action and Milestone (POA&M). SSPs are to be developed, documented, and periodically updated. A detailed roadmap of this process can be found in the AO SOP.

3 ATO PACKAGE REVIEW AND ACCEPTANCE PROCESS

3.1 ATO Package Review Post Assessment Phase
Detailed steps for the ATO Post Assessment Phase may be found in the Security Control Assessment (SCA) SOP uploaded on ConnectED. ATO packages will be submitted via SharePoint workflow by the Security Assessment Team (SAT) to the Department CISO for final review and concurrence. The detailed requirements of a complete ATO package may be found in the AO SOP.

3.2 ATO Package Review and Acceptance Process
The ATO review and approval process authorizes operation of an information system and explicitly accepts any documented and calculated risks to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation, based on the implementation of an agreed-upon set of security and privacy controls. Authorization also applies to common controls inherited by agency information systems and provides the objectives for the security control assessment. The AO provides detailed documentation for this process.

4 DELEGATION OF AO RESPONSIBILITIES FOR LOW IMPACT SYSTEMS
As directed through the CIO’s AO delegation memo, AO responsibilities for low impact systems have been delegated to respective Principal Office (PO) officials who wish to fulfill that role in their principal office. This delegation may not be delegated further without an updated memo to be approved by the department AO. Authorizing Officials must be Senior Executives or equivalent.
Authorizing officials must also adhere to all requirements stated in the delegation memo or risk having their authorizing authority reclaimed by the Department CIO.

5 **APPOINT OR REPLACE THE ISO FOR ALL SYSTEMS UNDER AO AUTHORITY**

If there is a need to appoint a new ISO or replace the existing ISO for any of systems under the AO’s authority, all applicable steps must be followed as documented in the AO SOP.

6 **AO Approval of Accepted Risk**

The Risk Acceptance Process is detailed in the Plan of Action and Milestones (POA&M) Standard Operating Procedures (SOP). All Department Risk Acceptance Forms (RAF) must be approved according to the residual risk level and system impact (FIPS 199 security categorization). The Risk Acceptance Process is outlined in the AO Acceptance SOP showing the AO responsibility in reviewing and approving the RAFs.

7 **RISK ACCEPTANCE/POLICY EXCEPTIONS**

Deviations from the Department policies, Instructions, Standards, Procedures or Memos must be approved and documented through the Department’s Risk Acceptance process. Deviations that introduce additional risks to the enterprise must be submitted through the Department Risk Acceptance Form (RAF) and must be approved by the ED CISO (as delegated). Requests must justify the reason for the deviation(s)/exception(s) as well as the compensating security controls implemented to secure the device or information, if applicable. Policy deviations that do not introduce additional risks do not need to be submitted through the Department RAF but will need to be approved by the Department CISO (as delegated).
8 APPENDIX A: ACRONYMS

AO  Authorizing Official
ATO  Authority to Operate
CPO  Chief Privacy Officer
CISO  Chief Information Security Officer
COR  Contracting Officer’s Representative
CSAM  Cyber Security Assessment and Management
ED  U.S. Department of Education
ETS  Enterprise Technology Services
FIPS  Federal Information Processing Standards
FISMA  Federal Information Security Modernization Act
GSS  General Support System
HVA  High Value Assets
IAS  Information Assurance Services
ISO  Information System Owner
ISSM  Information System Security Manager
ISSO  Information Systems Security Officer
ITS  Information Technology Services
MFR  Memo for the Record
NIST  National Institute of Standards and Technology
OCIO  Office of the Chief Information Officer
OIG  Office of Inspector General
OMB  Office of Management and Budget
PO  Principal Office
POA&M  Plan of Action and Milestones
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAF</td>
<td>Risk Acceptance Form</td>
</tr>
<tr>
<td>RRR</td>
<td>Residual Risk Report</td>
</tr>
<tr>
<td>SAOP</td>
<td>Senior Agency Official for Privacy</td>
</tr>
<tr>
<td>SAR</td>
<td>Security Assessment Report</td>
</tr>
<tr>
<td>SAT</td>
<td>Security Assessment Team</td>
</tr>
<tr>
<td>SCA</td>
<td>Security Controls Assessor</td>
</tr>
<tr>
<td>SOP</td>
<td>Standard Operating Procedure</td>
</tr>
<tr>
<td>SP</td>
<td>Special Publication</td>
</tr>
<tr>
<td>SSP</td>
<td>System Security Plan</td>
</tr>
</tbody>
</table>