# **acr2_logoLg.pngOne Hour DOD Cybersecurity Compliance: System Security Plan (SSP) and Action Plan (POAM) Updating Worksheet**

**Summary**

New DOD cybersecurity requirements for technical proposals mandate the creation and updating of System Security Plans (SSPs) that conform to the 110 specifications of NIST Special Publication 800-171. Creation of the SSP documentation is estimated (optimistically) by the government to “average 110 hours per response”. Using modified and updated bank cybersecurity software, ACR 2 Solutions has been able to reduce the labor required for initial SSP documentation to less than 30 hours for dozens of small DOD contractors. SSP updates, which use this Worksheet, typically require 1-2 hours of effort. The modified bank cybersecurity software is hosted on the FedRAMP compliant AWS portal www.cybercomplianceinthecloud.com.

**2018 DOD Cybersecurity Requirements**

The November 2018 Guidance for DOD on “Assessing Compliance of and Enhancing Protections for a Contractor’s Internal Unclassified Information System” begins on page 1 by requiring that, during solicitation and source selection, the Contractor "self-attests to compliance with DFARS 252.204-7012 and implementation of NIST SP 800-171.” The Guidance goes on in page 2 to require pre-award submittal of “the contractor’s system security plan… (NIST SP 800-171 Security Requirement 3.12.4), and any associated plans of action (NIST SP 800-171 Security Requirement 3.12.2). Requirements 3.12.4 and 3.12.2 are quoted below.

3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.

Page 7 of the Guidance notes that the “SSP and Plans of Action submissions, initial and subsequent, are submitted upon request. Requests will indicate what specific information is required (e.g., list of requirements not yet met and associated plans of action; description of how all requirements are met and associated plans of action)”. Page 7 goes on to claim, perhaps optimistically, that “Public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information.”

**General Instructions**

1. Replace all items in red with the information appropriate for your organization, deleting brackets and unused options as needed and render the text black.
2. Delete these instructions and all others in blue when you have finished with them.
3. Modify text in black, if appropriate, to add, modify or delete wording according to the needs of your organization.
4. Review document and ensure that all remaining text is in black.

**NIST 800-171 System Security Plan Report Guidance**

The requirements for NIST 800-171, including a system security plan, are detailed in the “NIST MEP

Cybersecurity Self-Assessment Workbook”. The System Security Plan (SSP) guidance below is taken from pages 122 and 123

*“There is no prescribed format or specified level of detail for system security plans. However, companies must ensure that the required information in 3.12.4 is appropriately conveyed in those plans…. System security plans describe how the company meets the security requirements, but do not provide detailed, technical descriptions of the specific design or implementation. System security plans contain sufficient information to enable a design and implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk to company operations and assets, employees, and other organizations, if the plan is implemented as intended.*

***System security plans need not be single documents****. The plans can be a collection of various documents including documents that already exist within the company. Effective systems security plans make* ***extensive use of references to policies, procedures, and additional documents*** *including, for example, design and implementation specifications where more detailed information can be obtained. This reduces the documentation associated with security programs and maintains the security-related information in other established management and operational areas including, for example, enterprise architecture, system development life cycle, systems engineering, and acquisition.”*

**Assembling the Updated SSP**

As allowed by NIST guidance, the updated SSP is largely composed of a collection of existing contractor cybersecurity records, revised as needed for each DOD technical proposal. Begin the updated SSP by logging in to [www.cybercomplianceinthecloud.com](http://www.cybercomplianceinthecloud.com) using credentials from your copy of the ACR 2 Cybersecurity Risk Management System™ (ACRMS™).

**Site and System Description**

Browse to the Document Management Center and open the Site Data Form and the most recent copy of Policy 3.4.1 3.4.2 Baseline Configuration. It should include the most recent network scan. This will address the 3.12.2 requirements to “describe system boundaries, system environments of operation…and the relationships with or connections to other systems. Read and review the documents for accuracy and make any necessary updates.

Save the updated documents as “SSP Update Site Name Date Appendix 1 Site Data.pdf” and “SSP Update Site Name Date Appendix 2 Network Data.pdf”. Save a working copy of this Worksheet document as “SSP Update Overview Site Name Date.doc”.

**Inventory of Safeguards**

Browse to Main Menu and click on the line “NIST 800-171 Compliance Report” as shown at right. This will bring up an HTML listing of all 110 NIST 800-171 requirements, their current status (Yes, No, Yes/Alt, NA or Partial) and the associated NIST 800-53 safeguards with their status. This meets the highlighted 3.12.4 requirement.

3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, **how security requirements are implemented**, and the relationships with or connections to other systems.

On the HTML page, click on “Export to Word Format” to create a status summary in .doc form. Formatting in portrait mode creates a 20 page inventory of the status of all 110 800-171 safety controls. Note that any safeguards marked NA (Not Applicable) or Yes/Alt (satisfied using an Alternate Solution) will typically require approval by your Contact Officer unless such approval was previously obtained and documented during a prior negotiation or contract. Save the word .doc file as a pdf with the name SSP Update Site Name Date Appendix 3 Safeguards Status.pdf

**Updated POAM**

Return to the Main Menu and click on the line “Gap Remediation Report – POAM”. When the HTML

listing of missing safeguards comes up, click on the “Edit Draft” button to bring up the screen below.

Each missing safeguard, listed in order of impact on RA-3 cybersecurity scores, has an NIST 800-53 title, a Responsible Party, a Target Date, a Status Summary and a Current Status. Any changes or updates may be made directly from this page or by using the Manage Assessment page initially used to enter safeguards information. Save any changes by clicking the Update button at the bottom of the page.

On the HTML “Edit Draft” page, click on “Export to Word Format” to create a POAM Report in .doc form. Save the word .doc file as a pdf with the name SSP Update Site Name Date Appendix 4 POAM Report.pdf.

**Updated Cybersecurity Risk Assessment**

Return to the Main Menu and select either “Start a New Update Assessment” or “[Complete Open Assessment](https://www.cybercomplianceinthecloud.com/acr2/SelectCategory.php?category=Review&assessment=10-26-18-1540558778&PHPSESSID=3jmhdbcmr3numt9hu3di6krhi4)”, whichever is live. At the bottom of the next page, click on “Manage Assessment” to bring up the data input page, as shown below.

Review the safeguards data and confirm acceptance. At the bottom of the page, as shown at right, Update any UTM and demographic information. Click on “Submit and Finalize Answers” to generate a new risk assessment.

The risk assessment report package will be sent by email to the compliance officer of record.

Open the PDF labeled “chart\_NIST Security” Copy the chart into this Worksheet using a snipping tool. An example is shown on the following page..

**Finalizing the Updated SSP**

1. Cut and paste the red Worksheet filename below this line. Turn to black.
2. Cut and paste the red appendix file names below the following title. Turn to black.

Supporting Documentation

1. Fill out the questionnaire, date and sign.
2. Erase all the blue text and blue circled figures.
3. Save the .doc file as pdf.

**System Security Plan Update Questionnaire**

After completion of the Site Security Plan report, it is recommended that the Security Plan Compliance Questionnaire be completed, signed and dated. A blank form is included on the following pages.

Date of SSP Update\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Are system security plans consistent with the organization’s enterprise architecture? (mark all that apply)

 Yes No Does Not Apply Alternative Approach

Does the system security plan explicitly define the authorization boundary for the system?

 Yes No Does Not Apply Alternative Approach

Does the system security plan describe the operational context of the system in terms of missions and business processes?

 Yes No Does Not Apply Alternative Approach

Does the system security plan describe the operational environment for the system?

 Yes No Does Not Apply Alternative Approach

Does the system security plan describe relationships with or connections to other systems?

 Yes No Does Not Apply Alternative Approach

Does the system security plan provide an overview of the security and privacy requirements for the system?

 Yes No Does Not Apply Alternative Approach

Does the system security plan describe the security requirements in place?

 Yes No Does Not Apply Alternative Approach

Does the system security plan include plans for meeting those requirements not yet in place?

 Yes No Does Not Apply Alternative Approach

Is the system security plan reviewed and approved by company management prior to plan implementation?

 Yes No Does Not Apply Alternative Approach

Are copies of the system security plan distribute to relevant company employees?

 Yes No Does Not Apply Alternative Approach

Are changes to the system security plan communicated to relevant company employees?

 Yes No Does Not Apply Alternative Approach

Does the company periodically review the system security plan within a certain timeframe? (e.g. annually)

 Yes No Does Not Apply Alternative Approach

Does the company update the system security plan to address changes to the system, environment of operation or problems identified during plan implementation or security assessments?

 Yes No Does Not Apply Alternative Approach

Does the company protect the system security plan from unauthorized disclosure and modification?

 Yes No Does Not Apply Alternative Approach

Does the company plan and coordinate security-related activities affecting the system before conducting any such activities?

 Yes No Does Not Apply Alternative Approach

Are security-related activities planned to reduce the impact on other company entities?

 Yes No Does Not Apply Alternative Approach

Questionnaire completed by: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 Print Name

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 Signature

Remember to erase all explanatory blue text.