

# CO/COR Cyber Guidance

## Contents of this Page

- [Pre-solicitation Questionnaire](#)
- [Pre-solicitation Review](#)
- [Pre-award Review](#)
- [Points of Contact](#)

## Overview

The NCI Information System Security Officer (ISSO) is part of the review process for acquisitions to evaluate if federal cybersecurity (FISMA, FedRAMP, etc.) language needs to be included in the statement of work (SOW) for an upcoming request for proposal (RFP).

To complete this review there are three steps:

1. Completing the **pre-solicitation questionnaire** in the RFP development process.
2. Completing the **pre-solicitation checklist** and review process prior to the RFP being released.
3. Completing the **pre-award checklist** and review process prior to the contract being awarded.

## Pre-solicitation Questionnaire

The pre-solicitation questionnaire gathers the required information for an upcoming RFP for the ISSO, to they can best assist the CO/COR in developing requirements for security.

Please see the link to the ISSO Pre-solicitation Questionnaire below:

[ISSO Pre-solicitation Questionnaire](#)

## Pre-solicitation Review

In doing the Pre-sol review, the NCI ISSO makes determinations if:

- The acquisition involves one or more information technology (IT) systems
- If there is an IT system(s) involved, will it be a Federal system?
  - If there is a federal system involved, it will be subject to FISMA requirements
    - Answers what kind of data will the system create, process, store, transmit, or receive?
    - Determines preliminary categorization (impact level) of either Low, Moderate, or High
    - Where will the system be hosted?
  - If not, then no FISMA requirements apply, and the review is complete

Please see the link to the ISSO Pre-solicitation Checklist below:

[ISSO Pre-solicitation Checklist](#)

## Pre-award Review

The purpose of the pre-award review is for the ISSO to look at winning bidder's proposal to confirm that the awardee acknowledges the security work required by the contract and the awardee addresses how they are going to meet these requirements in a realistic, timely, and satisfactory manner.

Please see the link to the ISSO Pre-award Checklist below:

[ISSO Pre-award Checklist](#)

## Points of Contact

For **Pre-solicitation and Pre-award** questions, comments, or concerns please contact:

Name	Phone Number	Email Address	Role
Blaise Czekalski*	(301) 480-4216	<a href="#">NCI IT Acquisition Security Review</a>	Primary Reviewer
Craig Hayn*	(240) 276-5159	<a href="#">NCI IT Acquisition Security Review</a>	1st Alternate

Karen Friend*	(240) 276-5055	<a href="#">NCI IT Acquisition Security Review</a>	2nd Alternate
---------------	----------------	--	---------------

\*as pre-solicitation and pre-award processes are inherently governmental and acquisitions sensitive, these individuals are Federal Employees and the NCI IT Acquisition Security Review email distribution list only contains Federal Employees.

For **Post-award** questions, comments, or concerns with regard to security-related deliverables and their review, please contact:

Name	Phone Number	Email Address	Role
Ann Pisz <sup>+</sup>	(240) 276-5209	<a href="mailto:NCICBIITSecurity-Governance@mail.nih.gov">NCICBIITSecurity-Governance@mail.nih.gov</a>	Cyber Governance, Risk, and Compliance Team Lead

<sup>+</sup>The Cyber Governance, Risk, and Compliance Team is made completely up of Contractors, and the NCI Cyber Governance, Risk, and Compliance Team email distribution list only contains Contractor staff. As such, never send any pre-award documentation (to include pre-solicitation) to any individual listed here or to the NCI Cyber Governance, Risk, and Compliance Team email distribution list.