

Name of Offeror		
	Answer (Y;N;I; or NA) see Legend below	Information see Legend below
Does your organization limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems)?		
Does your organization limit information system access to the types of transactions and functions that authorized users are permitted to execute?		
Does your organization verify and control/limit connections to and use of external information systems?		
Does your organization control information posted or processed on publicly accessible information systems?		
Does your organization identify information system users, processes acting on behalf of users, or devices?		
Does your organization authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems?		
Does your organization sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse?		
Does your organization limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals?		
Does your organization escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices?		
Does your organization monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems?		
Does your organization implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks?		
Does your organization identify, report, and correct information and information system flaws in a timely manner?		
Does your organization provide protection from malicious code at appropriate locations within organizational information systems?		
Does your organization update malicious code protection mechanisms when new releases are available?		
Does your organization perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed?		
I understand that a response of "no" to any of the items above disqualifies my organization from receiving a SEWP VI Contract award. I hereby certify that, to the best of my knowledge, the provided information is true and accurate. (Signature Required)		
First and Last Name of Signer		
Date of signature		
	Legend	Type of information required.
	Y=Yes/fully compliant	None
	N=Not compliant	None
	I=In Progress	Indicate extent of progress
	NA=Not Applicable	Indicate why this is Not Applicable