29. NAME (*Last, First, Middle Initial*)	29a. SOCIAL SECURITY NUMBER (LAST FOUR)

30. USER RESPONSIBILITIES

I understand that to ensure the integrity, safety and security of Navy IT resources, when using those resources, I shall:

- Safeguard information and information systems from unauthorized or inadvertent modification, disclosure, destruction, or use.
- Protect Controlled Unclassified Information (CUI) and classified information to prevent unauthorized access, compromise, tampering, or exploitation of the information.
- Protect passwords for systems requiring logon authentication and safeguard passwords at the sensitivity level of the system for classified systems and at the confidentiality level for unclassified systems. Passwords will be classified at the highest level of information processed on that system.
- Virus check all information, programs, and other files prior to uploading onto any Navy IT resource.
- Report all security incidents immediately in accordance with local procedures and CJCSM 6510.01 (series).
- Access only that data, control information, software, hardware, and firmware for which I am authorized access and have a need-to-know, and assume only those roles and privileges for which I am authorized.

I further understand that, when using Navy IT resources, I shall not:

- Access commercial web-based e-mail (e.g. HOTMAIL, YAHOO!, AOL, etc.)
- Auto-forward official e-mail to a commercial e-mail account.
- Bypass, strain, or test IA mechanisms (e.g., Firewalls, content filters, anti-virus programs, etc.). If IA mechanisms must be bypassed, I shall coordinate the procedure and receive written approval from the Local IA Authority (CO or OIC).
- Introduce or use unauthorized software, firmware, or hardware on any Navy IT resource.
- Relocate or change equipment or the network connectivity of equipment without authorization from my Local IA Authority.
- Use personally owned hardware, software, shareware, or public domain software without authorization from the Local IA Authority.
- Upload executable files (e.g., .exe, .com, .vbs, or .bat) onto Navy IT resources without the approval of the Local IA Authority.
- Participate in or contribute to any activity resulting in a disruption or denial of service.
- Write, code, compile, store, transmit, transfer, or introduce malicious software, programs, or code.
- Put Navy IT resources to uses that would reflect adversely on the Navy (such as uses involving pornography; chain letters; unofficial advertising, soliciting or selling except on authorized bulletin boards established for such use; violation of statute or regulation; inappropriately handled classified information; and other uses that are incompatible with public service).

31. USER SIGNATURE	32. DATE

PART III - SECURITY MANAGER VALIDATES THE BACKGROUND INVESTIGATION OR CLEARANCE INFORMATION

33. TYPE OF INVESTIGATION		33a. DATE OF INVESTIGATION (YYYYMMDD)	
33b. CLEARANCE LEVEL		33c. IT LEVEL DESIGNATION ☐ LEVEL 1 ☐ LEVEL 2 ☐ LEVEL 3	
34. VERIFIED BY *(Print name)*	35. SECURITY MANAGER TELEPHONE NUMBER	36. SECURITY MANAGER SIGNATURE	37. DATE (YYYYMMDD)

PART IV - COMPLETION BY AUTHORIZED STAFF PREPARING ACCOUNT INFORMATION

38. TITLE:	38a. SYSTEM	38b. ACCOUNT CODE
	38c. DOMAIN	
	38d. SERVER	
	38e. APPLICATION	
	38f. DIRECTORIES	
	38g. FILES	
	38h. DATASETS	
39. DATE PROCESSED (YYYYMMDD)	39b. PROCESSED BY (*Print name and sign*)	39c. DATE (YYYYMMDD)
40. DATE REVALIDATED (YYYYMMDD)	40a. REVALIDATED (*Print name and sign*)	40b. DATE (YYYYMMDD)