SECURITY INSPECTION CHECKLIST	YES	NO	N/A	DON'T KNOW
PART I **PROGRAM MANAGEMENT**				
1. Does the command hold the current edition of SECNAVINSTs 5510.36A and 5510.30B and SECNAV Manuals M-5510.36 and 5510.30?				
2. Does the command hold the references applicable to its security program?				
3. Is the command in possession of the following classified information references (if applicable?				
a. COMSEC, EKMS-1?				
b. DOD SCI Security Manual/relevant DCIDs?				
c. SAPs, OPNAVINST S5460.3(series)?				
d. NC2 OPNAVINST S5511.35(series)?				
e. NNPI, NAVSEAINST C5511.32(series)?				
f. RD/FRD, DOD Directive 5210.2?				
g. CNWDI, DOD 5210.2?				
h. NATO, OPNAVINST C5510.101(series)?				
i. Classified information released to industry, NISP?				
4. Are waivers or exceptions submitted to the CNO (N09N2) for all conditions that prevent compliance with SECNAVINSTs?				
PART II **COMMAND SECURITY MANAGEMENT**				
5. Is the security organization in the command defined?				
6. Has the Commanding Officer:				
a. Issued a command security instruction?				
b. Approved an emergency plan for the protection and destruction of classified information?				
c. Established an Industrial Security Program?				
d. Ensured that the security manager and other personnel have received security education and training?				
e. Ensured that personnel are evaluated on the handling, creation or management of classified information on performance evaluations?				
7. To implement the ISP and PSP, has the commanding				

		YES	NO	N/A	DON'T KNOW
	officer designated in writing:				
	a. Security manager?				
	b. TSCO? (If applicable)				
	c. TSCA? (If applicable)				
	d. Assistant security manager?				
	e. Security assistant(s)?				
	f. EKMS Manager and alternate? (If applicable)				
	g. NWP custodian? (If applicable)				
	h. NATO control officer and alternate? (If applicable)				
	i. One or more CORs (If applicable)				
8.	Has the Security Manager's designation letter been forwarded to CNO (N09N2)?				
9.	Has the Security Manager been formally trained?				
10.	How many persons are assigned duties and responsibilities to support the command's security program, what are their duties and how do they report to the security manager?				
11.	Is the command security manager named and identified to command personnel on command organizational charts, telephone listings, rosters, or other media?				
12.	Does the security manager have direct and ready access to the appointing official?				
13.	Is the security manager exercising overall management of the program?				
14.	Does the security manager have sufficient authority and staff to function effectively?				
15.	Do the SSO, IAM, and security manager coordinate and cooperate in the command program?				
16.	Has the command security manager:				
	a. Developed a command security instruction?				
	b. Formulated, coordinated, and conducted a command security education program?				
	c. Kept command personnel abreast of all changes in security policies and procedures?				
	d. Reported and investigated all security threats and compromises?				
	e. Promptly referred all incidents to NCIS under				

	YES	NO	N/A	DON'T KNOW
their jurisdiction?				
f. Coordinated the preparation of the command SCGs?				
g. Maintained liaison with the PAO on proposed media releases?				
h. Developed security procedures for visitors who require access to classified information?				
i. Implemented regulations concerning the disclosure of classified information to foreign nationals?				
17. Does the TSCO manage and control all command TS information, less SCI?				
18. Are security functions performed by another command covered by a written Security Servicing Agreement?				
19. Have qualified security inspectors conducted command inspections, assist visits, and program reviews to examine the command's overall security posture?				
20. Does the command inspect and evaluate subordinate commands?				
21. Do inspections include evaluation of subordinate commands security programs?				
22. Are qualified inspectors used?				
23. Are inspection and any follow-up reports on file?				
PART III SECURITY EDUCATION AND TRAINING				
24. Does the command have an effective security education program?				
25. Does the command hve any command generated or designed security awareness or education plans?				
26. Were security education materials coordinated with CNO (N09N2) (if required)				
27. Is additional training provided to:				
a. Approved OCAs and their officially "acting" alternates?				
b. Derivative classifiers, security managers, and other security personnel?				
c. Classified couriers?				
d. Declassification authorities?				
28. Are indoctrination briefings given?				

		YES	NO	N/A	DON'T KNOW
29.	Are orientation briefings given?				
30.	Is on-the-job training given?				
31.	Are annual refresher briefings given?				
32.	Are counterintelligence briefings given?				
33.	Are foreign travel briefings given?				
34.	Have all personnel with SIPRNET NATO, NC2, or CNWDI access been briefed as required?				
35.	Has attestation been completed for each person at the command with TS, SCI and or SAP eligibility?				
36.	Are copes maintained off any reports made to appropriate CI, investigative and personnel security authorities concerning any employee know to have been responsible for repeated security violations				
37.	Do procedures ensure the Security Termination Statement is executed when required?				
	PART IV CLASSIFICATION MANAGEMENT				
38.	Is information classified only to protect national security information?				
39.	Do procedures prohibit the use of terms such as "FOUO" or "Secret Sensitive" for the identification of classified information?				
40.	Have the command OCAs been trained in their duties and responsibilities?				
41.	Has written confirmation of this training (i.e., indoctrination letter) been submitted to the CNO (N09N2)?				
42.	Is information that has been released to the public without proper authority classified or reclassified only when the information can be reasonably recovered, most individual holders are known, and is it withdrawn from public access?				
43.	Is the classification level, of any information believed to be improperly classified, challenged?				
44.	Does NATO and FGI retain its original classification level and are assigned an U.S. classification equivalent, if necessary?				
45.	Are procedures established for initial response to command mandatory declassification reviews within 45 working days?				
46.	Are reasonable steps taken to declassify information determined to be of permanent historical value prior				

		YES	NO	N/A	DON'T KNOW
	to their accession into NARA?				
47.	Have cognizant OCA(s) notified holders of unscheduled classification changes involving their information?				
	PART V SECURITY CLASSIFICATION GUIDES				
48.	Is a SCG issued for each classified system, program, plan, or project as soon as practicable before the initial funding or implementation of the system, program, plan, or project?				
49.	Is each SCG approved personally and in writing by an OCA who has program or supervisory responsibility over the information?				
50.	Are command SCGs formatted per OPNAVINST 5513.1 (series)?				
51.	Are Command-originated SCGs reviewed, by the cognizant OCA, at least every 5 years?				
52.	Are all changes promptly submitted to the Rankin Program Manager (CNO (N09N2)?				
	PART VI MARKING CLASSIFIED INFORMATION				
53.	Are all classified documents and their portions properly marked to include all applicable basic and associated markings?				
54.	Are originally classified documents marked with a "Classified by" and "Reason" line?				
55.	Are derivatively classified documents marked with a "Derived from" line?				
56.	Is "Multiple Sources" annotated on the "Derived from" line of classified documents derived from more than one source?				
57.	Is a source listing attached to the file copy of all documents classified by "Multiple Sources"?				
58.	Are downgrading and declassification instructions included on all classified documents, less exception documents?				
59.	Are the appropriate warning notices placed on the face of classified documents				
60.	Are classified intelligence documents/portions marked with the appropriate intelligence control marking(s)?				
61.	Is the face of NATO and Foreign Government RESTRICTED documents and FGI marked with the				

		YES	NO	N/A	DON'T KNOW
	appropriate notice?				
62.	Are the portions of documents containing NATO and FGI marked to indicate their country of origin?				
63.	Is the assignment and use of nicknames, exercise terms and code words per OPNAVINST 5511.37C**?**				
64.	Is an explanatory statement included on the face of documents classified by compilation?				
65.	Do documents, marked classified for training and test purposes, include a statement indicating that the documents are actually unclassified?				
66.	When removed or used separately are component parts of classified documents marked as separate documents?				
67.	Are letters of transmittal marked to show the highest overall classification level of any information being attached or enclosed?				
68.	Are electronically transmitted messages properly marked?				
69.	Are classified files or folders marked or have the appropriate SFs been attached to indicate the highest overall classification level of the information contained therein?				
70.	Are all classified materials such as IT media, maps, charts, graphs, photographs, briefing slides, recordings, and videotapes appropriately marked?				
71.	Are all classified emails sent over security IT systems marked as required?				
	PART VII SAFEGUARDING				
72.	Does the command ensure that all DON employees (military and civilian) who resign, retire, separate or are released from active duty return all classified material in their possession?				
73.	Is TS information, including copies, originated or received by the command, completely identified accounted for, individually serialized, and entered into the command's TS inventory?				
74.	Are command TS documents and material physically sighted at least annually?				
75.	Does the command have control measures in place for receipt and dispatch of Secret information?				
76.	Are control measures in place to protect the unauthorized access to command TS, Secret, or Confidential information?				

		YES	NO	N/A	DON'T KNOW
77.	Are working papers:				
	a. Dated when created?				
	b. Marked "Working Paper" on the first page?				
	c. Marked with the highest overall classification center top and bottom of each applicable page?				
	d. Destroyed when no longer needed?				
	e. Controlled and marked after 180 days or when they are released outside the command?				
78.	Are appropriate control measures taken for other special types of classified information?				
79.	Are SFs 703, 704,and 705 placed on all classified information when removed form secure storage?				
	a. Are SFs 706, 707, 708, and 712 being utilized on classified IT system media, when feasible?				
	b. When SF media labels are not feasible due to the size of the media or interference with media operation, are other methods for identifying the classification of the media used?				
	c. Are classified typewriter ribbons, carbon sheets, plates, stencils, drafts, and notes controlled, handled, and stored per their classification level?				
80.	Has the command established procedures for end of the day security checks, to include the use of the SFs 701 and 702?				
81.	Are classified vaults, secure rooms, and containers made an integral part of the end of the day security check?				
82.	Are procedures in place to ensure that visitors have access only to information to which they have a need-to-know and the appropriate clearance eligibility?				
83.	Are procedures in place for classified meetings held at the command or hosted by cleared facilities?				
84.	Is classified information reproduced only to the extent that is mission essential?				
	PART VIII DISSEMINATION OF CLASSIFIED INFORMATION				
85.	Are procedures established to ensure the proper dissemination of classified information outside DOD and foreign governments?				
86.	Are special types of classified information and controlled unclassified information disseminated per				

		YES	NO	N/A	DON'T KNOW
	their governing instructions?				
87.	Is information disseminated to Congress per SECNAVINST 5730.5 (series) and OPNAVINST 5510.158 (series)?				
88.	Do all newly generated classified and unclassified technical documents include a distribution statement listed in exhibit 8A of SECNAV M-5510.36?				
89.	Is unclassified technical data which reveals critical technology with military or space application and requires an approval, authorization, or license for its lawful export withheld from public disclosure per OPNAVINST 5510.161?				
90.	Is command information intended for public release, including information released through IT systems (i.e., INTERNET, computer servers), submitted for prepublication review?				
	PART IX TRANSMISSION AND TRANSPORTATION				
91.	Is classified information transmitted or transported only per specific requirements?				
92.	Are special types of classified information transmitted or transported per their governing instructions?				
93.	Are command personnel advised not to discuss classified over unsecured circuits?				
94.	Are command procedures established for preparing classified bulk shipments as freight?				
95.	Is classified information transported or transmitted outside the command receipted for?				
96.	Does the command authorize the handcarry or escort of classified information, via commercial aircraft, only if other means are not available and there is an operational or contractual requirement?				
97.	Are designated couriers briefed on their courier responsibilities and requirements?				
98.	Are procedures established for the control and issuance of the DD 2501?				
	PART X STORAGE AND DESTRUCTION				
99.	Are any command weaknesses, deficiencies or vulnerabilities in any equipment used to safeguard classified information reported to the CNO (N3AT)?				
100.	Does the command ensure that weapons, money, jewelry or narcotics are not stored in the same security				

		YES	NO	N/A	DON'T KNOW
	container used to store classified information?				
101.	Does the command ensure that external markings on command security containers do not reveal the level of information stored therein? **(ISP 10-1)**				
102.	Does command security equipment meet the minimum standards of GSA?				
103.	Does the command meet the requirements for the storage of classified bulky information?				
104.	Does the command mailroom have a GSA-approved security container to store USPS First Class, Certified and Registered mail and commercial express deliveries overnight?				
105.	Are command vaults and secure rooms, not under visual control at all times during duty hours, equipped with electric, mechanical or electro-mechanical access control devices?				
106.	Are specialized security containers securely fastened to the structure, rendering them non-portable?				
107.	Has the command disposed all containers manufactured by Remington Rand and disqualified containers manufactured by Art Metal Products, Inc.?				
108.	Is classified information removed from the designated work areas for work at home done so only with prior approval of appropriate officials?				
109.	Are command container combinations changed:				
	a. By individuals who possesses the appropriate clearance level?				
	b. Whenever the container is first put into use?				
	c. Whenever an individual knowing the combination no longer requires access to the container (unless other sufficient controls exist to prevent access)?				
	d. Whenever a combination has been subjected to possible compromise?				
	e. Whenever the container is taken out of service?				
110.	Are command container combinations marked and accounted for per the classification level of the information stored therein?				
111.	Is there a SF 700 affixed inside each command security container?				
112.	Does the SF 700 include the names, home addresses and phone numbers of persons to be contacted if the				

		YES	NO	N/A	DON'T KNOW
	container if found open and unattended?				
113.	Is the combination placed in the SF 700, and is it properly secured in an appropriate security container?				
114.	Has the command established procedures for command key and padlock accountability and control?				
115.	Are command locks repaired by only authorized personnel, who have been subject to a trustworthy determination or who are continuously escorted?				
116.	Are command security containers, previously placed out of service, marked as such on the outside and the "Test Certification Label" removed on the inside?				
117.	Are command security containers with visible repair results, marked as such with a label posted inside the container stating the details of the repairs?				
118.	Are all commercial IDSs used on command security containers, vaults, modular vaults, and secure rooms, approved by the CNO (N3AT)?				
119.	Is command classified information destroyed when no longer required?				
120.	Do all command shredders, pulverizes, and disintegrates meet the minimum requirements?				
121.	Is the command replacing old shredders or those that need repair with shredders that meet the new NSA Standards?				
122.	Has the command established effective procedures for the destruction of classified information?				
123.	When filled, are command burn bags sealed and safeguarded per their highest overall classification level of their contents?				
124.	Is controlled unclassified information destroyed per their governing instructions?				
	PART XI INDUSTRIAL SECURITY PROGRAM				
125.	Has the command established an Industrial Security Program?				
126.	Has the command imposed any Program Protection Plans (PPPs) on its contractors via the contract?				
127.	Has the commanding officer established or coordinated oversight over classified work carried out by cleared contractor employees in spaces controlled or occupied at DON shore commands?				

	YES	NO	N/A	DON'T KNOW
128. Does the command COR:				
a. Complete, issue, and sign all DD 254s?				
b. Validate all contractor security clearances?				
c. Verify contractor storage capability prior to authorizing release of classified information?				
d. Provide additional security requirements via the contract or DD 254?				
e. Review all reports of industry security violations and forward to program managers?				
f. Coordinate DD 254 reviews and guidance, as needed?				
g. Verify that cleared DOD contractor employees who are used as couriers have been briefed on their courier responsibilities?				
129. Have all FADs been issued per SECNAV M-5510.36?				
130. Is classified intelligence information disclosed only to those contractors cleared under the NISP and as authorized on the DD 254?				
PART XII LOSS AND ACTUAL OR POSSIBLE COMPROMISE OF CLASSIFIED INFORMATION				
131. Is the command security manager responsible for overseeing the response to all losses or compromises of classified information, including those that occurred on IT systems?				
132. Since the last inspection, has the command had any incidents involving a loss and or compromise of classified information?				
133. If a possible loss or compromise occurred, was a PI conducted?				
134. If a significant command weaknesses, if disciplinary action is contemplated, or a confirmed or probable loss or compromise occurred, was a JAGMAN investigation conducted?				
135. When the loss or compromise of classified information or equipment has occurred, is appropriate investigative and remedial action(s) taken to ensure further loss or compromise does not recur?				
136. Is appropriate and prompt corrective action taken whenever a knowing, willful, or negligent compromise occurs or repeated administrative disregard of security regulations occurs?				
137. Are procedures established for review of				

		YES	NO	N/A	DON'T KNOW
	investigations by seniors?				
138.	Are security reviews conducted on information subjected to loss or compromise?				
139.	Are procedures established for classification reviews by originators or OCAs?				
140.	Is receipt of improperly transmitted information reported to the sender?				
141.	Are military and civilian personnel made aware that they are subject to administrative sanctions for knowingly, willfully, or negligently committing security violations				
142.	Are reports made to appropriate counterintelligence, investigative, and personnel security authorities concerning any employee who is known to have been responsible for repeated security violations?				
143.	Are counterintelligence matters reported to NCIS when required?				
144.	Have all personnel been advised of the requirement to report any contact with any individual regardless of nationality, in which unauthorized access is sought or personnel are concerned that they may be the target of exploitation by a foreign entity?				
145.	Are investigations conducted and counterintelligence reports made to NCIS where necessary in connection with unauthorized absentees?				
	PART XIII PERSONNEL SECURITY				
146.	If non-U.S. citizens are employed at command are security procedures in place to limit access?				
147.	Are non-U.S. citizens and others who are ineligible for access to classified information identified to other command personnel?				
148.	Does command have copies of IT position designations?				
149.	Are only U.S. citizens nominated for security clearance determinations?				
150.	Are only U.S. citizens assigned to sensitive duties?				
151.	Have policies concerning granting of access to non-U.S. citizens been adhered to?				
152.	Have the policies concerning the assignment of non-U.S. citizens to sensitive positions been adhered to?				
153.	Is CNO (N09N) approval obtained before appointment of non-U.S. citizens to civilian sensitive				

		YES	NO	N/A	DON'T KNOW
	positions?				
154.	Is U.S. citizenship verified before requesting personnel security investigations?				
155.	Have all civilian positions been designated by sensitivity?				
156.	Do any persons in command in non-sensitive positions have access to a DON IT system?				
157.	Are requests for Personnel Security Investigations kept to the minimum level of investigation necessary?				
158.	Is the prohibition against conducting PSIs locally being observed?				
159.	Is the proper investigation for civilian employment being requested?				
160.	Are PSIs requested only when necessary				
161.	Is the appropriate investigation for access or assignment being requested?				
162.	Are PSI requests prepared and submitted as required?				
163.	Is follow-up action taken when appropriate?				
164.	Are investigative reports controlled and safeguarded as required?				
165.	Is the filing of investigative reports in official personnel records strictly prohibited and such prohibition observed?				
166.	Is verification sought when there are indications a prior investigation could satisfy current needs?				
167.	Are security criteria and adjudication guidelines being applied in personnel security determinations?				
168.	Are records of personnel security determinations properly maintained?				
169.	Are adverse personnel security determination procedures being strictly observed?				
170.	Is there a program for continuous evaluation of eligibility for access or assignment to sensitive duties?				
171.	Are local record checks conducted and recorded?				
172.	Are command clearances and access determinations documented in JPAS				
173.	Are temporary access (interim security clearance) procedures followed?				

		YES	NO	N/A	DON'T KNOW
174.	Is access granted only to those eligible and documented in JPAS?				
175.	Are temporary accesses (interim clearances) properly granted and recorded in JPAS?				
176.	Is access to NATO and other special program access being recorded in JPAS?				
177.	Are denials or revocations of clearance processed as required?				
178.	Is access granted only to those with a need to know?				
179.	Are JPAS users controlled and monitored?				
180.	Are restrictions on access by non-U.S. citizens being observed?				
181.	Are personnel with established security clearance eligibility prohibited from gaining access to classified information until they have received an initial security briefing and signed a Standard Form 312, "Classified Information Nondisclosure Agreement"?				
182.	Are special accesses authorized by the command recorded?				
183.	Has one time access been granted and properly recorded?				
184.	Have any Limited Access Authorizations been issued by CNO (N09N)?				
185.	Is access by foreign nationals or visitors adequately controlled?				
	PART XIV INFORMATION ASSURANCE (IA)				
186.	Is an Information Assurance Manager (IAM) assigned?				
187.	Are the command's IT systems and networks accredited?				
188.	Do the Security Manager and IAM work closely together on issues related to classified information processing on IT systems?				
189.	Is command in compliance with DONs Web page policy?				
190.	Are all IT equipment and removable media properly marked				
191.	Has a policy on use of portable electronic devices been established for areas where classified information is processed or discussed				
192.	Are any spillages which result in compromise of classified material promptly investigated and				

	YES	NO	N/A	DON'T KNOW
reported				