

Chapter 2 – Standards of Conduct and Managers’ Internal Control Program (MICP)

Table of Contents

2.1	Introduction	2-3
2.2	Summary of Amended Procurement Integrity Act	2-3
2.3	Disclosing and Obtaining Procurement Information	2-4
2.3.1	Disclosing Procurement Information	2-4
2.3.2	Obtaining Procurement Information	2-4
2.4	Actions Required Regarding Offers of Non-Federal Employment	2-4
2.5	Post-Government Employment Restrictions	2-5
2.6	Determining Violations or Possible Violations	2-6
2.7	Measures to Minimize Improper Conduct	2-6
2.8	Hotline Policies and Procedures for NAVSEA Shore Activities	2-7
2.9	Fraud, Waste, and Other Abuse	2-8
2.9.1	Coordination for Fraud Prevention	2-8
2.9.2	Indicators of Defective Pricing Fraud	2-8
2.9.3	Actions against Fraudulent Activities	2-10
2.9.4	Government Personnel	2-11
2.10	Managers’ Internal Control Program (MICP)	2-11
	Appendix 2-A: SUPSHIP Managers’ Internal Control Program (MCIP) Manual	2-13
	Appendix 2-B: Acronyms	2-39

References

- (a) 5 CFR 2635, Standards of Ethical Conduct for Employees of the Executive Branch
- (b) DoD 5500.7-R, DoD Joint Ethics Regulations
- (c) 41 USC 421, Office of Federal Procurement Policy Act
- (d) PL 104-106, Amended Procurement Integrity Act
- (e) Federal Acquisition Regulations (FAR)
- (f) 18 USC 204, Restrictions on former officers, employees, and elected officials of the executive and legislative branches
- (g) 5 CFR 2641, Post-employment conflict of interest restrictions
- (h) DoD Directive 5500.07, DoD Standards of Conduct
- (i) NAVSEAINST 5041.1A, DoD Hotline Program Policy and Procedures for NAVSEA
- (j) DoDINST 7050.5, Coordination of Remedies for Fraud and Corruption Related to Procurement Activities
- (k) SECNAVINST 5430.92B, Assignment of Responsibilities to Counteract Acquisition Fraud, Waste, and Related Improprieties within the Department of the Navy
- (l) 31 USC 3729, Civil False Claims Act
- (m) 31 USC 3801, Program Fraud Civil Remedies Act
- (n) 41 USC 601-613, Contract Disputes Act
- (o) 18 USC 874, Anti-Kickback Act of 1986
- (p) 41 USC 605, Decision by contracting officer
- (q) 10 USC 2408, Prohibition on Persons Convicted of Defense Contract-Related Felonies and Related Criminal Penalty on Defense Contractors
- (r) 10 USC 2324, Allowable Costs Under Defense Contracts
- (s) OMB Circular A-123, Management's Responsibility for Internal Control
- (t) NAVSEAINST 5200.13C, Management Control Program (MCP)

Chapter 2 – Standards of Conduct and Managers’ Internal Control Program (MICP)

2.1 Introduction

Considering the significant power vested in Government officials, the public should expect the conduct of such officials to conform to the highest ethical standards. Congress has passed numerous ethics laws, and the Executive branch has promulgated Government-wide regulations addressing the standards of ethical conduct expected of Government employees, both military and civilian (see [5 CFR 2635](#), reference (a), Standards of Ethical Conduct for Employees of the Executive Branch and [DoD 5500.7-R](#), reference (b), the DoD Joint Ethics Regulations). As required by DoD for its employees, SUPSHIP personnel receive periodic ethics training from their local counsel’s office.

In the context of federal procurements, Congress enacted the Office of Federal Procurement Policy Act, [41 USC 421](#), reference (c). This law was amended by [Public Law 104-106](#), reference (d), and is referred to as the Amended Procurement Integrity Act.

2.2 Summary of Amended Procurement Integrity Act

[FAR 3.104](#), reference (e), implements section 27 of the Office of Federal Procurement Policy Act ([41 USC 423](#)). The effective date of the new law was 1 January 1997. The amended law focuses on:

- improperly releasing or obtaining source selection information and contractor bid or proposal information (formerly referred to as “proprietary information”)
- employment discussions between agency officials and contractors
- employment by contractors of former Government officials

These items will be discussed in more detail in later sections of this chapter.

The amended law eliminates all requirements for written certifications, e.g., certifications regarding familiarity with act; not being aware of violations; promising to disclose information about possible violations; and continuing obligation not to disclose proprietary and source selection information.

The amended law eliminates the prior prohibition on a “procurement official” soliciting or accepting a gratuity valued at more than \$10 from a “competing contractor” “during the conduct of a procurement.” This restriction was deemed to duplicate other gratuities rules, such as the prohibition in the Government-wide standards of conduct regarding gifts from prohibited sources in excess of \$20.

Further, the amended law eliminates the requirement for each agency to have a procurement ethics program for training its procurement officials.

2.3 Disclosing and Obtaining Procurement Information

2.3.1 Disclosing Procurement Information

The amended law prohibits certain persons from disclosing certain procurement information, i.e., contractor bid or proposal information or source selection information. This prohibition applies to any person who is:

- a present or former officer or employee of the United States
- any person who is acting or has acted on behalf of the United States
- anyone who has advised the United States with respect to a federal agency procurement and who, by virtue of his office, employment, or relationship, has access to bid, proposal, or source selection information

Such persons must not knowingly disclose such information before the award of the procurement to which the information relates. This section applies only to procurements using competitive procedures. The amended law provides for criminal penalties, including fines and imprisonment for up to five years, if the disclosure was made in exchange for money or to give anyone a competitive advantage.

Definitions relative to this prohibition, “source selection and proprietary information,” are essentially the same terms as prior to amending of the law. The term “contractor bid or proposal information” encompasses proprietary information.

2.3.2 Obtaining Procurement Information

The amended law also prohibits anyone from knowingly obtaining the procurement information described above. Specifically, no one will knowingly obtain such information before award. Mere solicitation of procurement information does not violate the amended law. The same criminal penalties apply to knowingly obtaining procurement information.

2.4 Actions Required Regarding Offers of Non-Federal Employment

If an agency official who is participating personally and substantially in a competitive procurement in excess of \$100,000 contacts or is contacted by a bidder or offeror regarding non-federal employment, he or she will give notice and disqualify him or herself from participating in the procurement, unless the possibility of employment is rejected.

The official must report this contact in writing to the immediate supervisor and to the Designated Agency Ethics Official (DAEO), or his designee (local counsel), and either reject the possibility of employment or disqualify himself/herself from further participation until authorized to resume participation. In contrast to the prior law, the disqualification is immediate.

A written notice of disqualification goes to the Head of the Contracting Activity (HCA) or his/her designee, with concurrent copies to the immediate supervisor, the contracting officer, the Source Selection Authority (SSA), and the local legal office. Copies of these disqualifications must be kept for two years.

FAR states that if an employee participates “personally and substantially” in certain listed procurement-related activities, then he/she will be required to report such contacts and either reject the possibility of employment or disqualify himself/herself. Participating personally and substantially in a federal procurement is defined in [FAR 3.104-1](#). Civil or administrative penalties can be imposed for violations of this prohibition.

2.5 Post-Government Employment Restrictions

The amended law provides for a one year prohibition on receipt of compensation from certain contractors if a former official served in certain capacities or made certain decisions on behalf of the Government. However, the amended law only applies to services provided or decisions made on or after 1 January 1997, the effective date of the amended law.

Individuals who left the Government prior to 1 January 1997 are not covered by the amended law but are subject to the old procurement integrity rules. However, the old procurement integrity rules do not apply to anyone after 31 December 1998.

Under the amended law, a former agency official may not accept compensation from a contractor within a period of one year after such official:

- Served as the Procuring Contracting Officer (PCO), SSA, member of the Source Selection Evaluation Board (SSEB), or the chief of a financial or technical evaluation team. This applies for a procurement in which the contractor was selected for award of a contract in excess of \$10 million.
- Served as the Program Manager, deputy Program Manager, or Administrative Contracting Officer (ACO) for a contract in excess of \$10 million awarded to the contractor.
- Personally made a decision to:
 - Award a contract, subcontract, modification of a contract or subcontract, or a task or delivery order in excess of \$10 million to the contractor
 - Establish overhead or other rates applicable to a contract or contracts for the contractor that are valued in excess of \$10 million
 - Approve issuance to the contractor of a contract payment or payments in excess of \$10 million
 - Pay or settle a claim with the contractor in excess of \$10 million

Civil or administrative penalties can be imposed on both the former official and the contractor for violations of this prohibition.

A former official is not prohibited from accepting compensation from any division or affiliate of a contractor that does not produce the same or similar products or services as the entity of the contractor that is responsible for the contract. This restriction applies to sole source and competitive contracts in excess of \$10 million.

Under the amended law, as under the old law, the DAEO (counsel) will give a safe harbor (i.e., ethics advisory) opinion to any employee or former employee who wishes to know whether the individual can accept compensation from a particular contractor subsequent to their separation from the Government.

In post-government employment restriction, the term “in excess of \$10 million” means the value of a contract, including the estimated value of the contract at the time of award, and all options.

In addition to the post-employment restrictions mentioned above, a criminal statute in [18 USC 204](#), reference (f), contains several post-employment restrictions that apply to certain former employees including a basic prohibition for all that “No former employee shall knowingly, with the intent to influence, make any communication to or appearance before an employee of the United States on behalf of any other person in connection with a particular matter involving a specific party or parties in which he participated personally and substantially as an employee and in which the United States is a party or has a direct and substantial interest,” ([5 CFR 2641](#), reference (g)). Employees should consult their ethics advisor for advice on specific post-employment restrictions that apply to them.

2.6 Determining Violations or Possible Violations

If the contracting officer receives or obtains information of a violation or possible violation of the law, that officer is required to determine whether it has an impact on the pending award or source selection. If the contracting officer determines that the violation or possible violation impacts the procurement, he/she is to forward this information to the HCA or his/her designee. The HCA who receives information that describes an actual or possible violation will review all relevant information and take appropriate action. The HCA may request information from appropriate parties about the violation. If the HCA determines that the Act has been violated, the HCA may direct the contracting officer to cancel the procurement, disqualify an offeror, or take other appropriate action.

2.7 Measures to Minimize Improper Conduct

Supervisory personnel should make the following available to all cognizant personnel: a copy of the [FAR, DoD Directive 5500.07](#) (Standards of Conduct), reference (h), and the [DoD Joint Ethics Regulation](#). Measures should be instituted to minimize prohibited conduct. SUPSHIP personnel must understand that violation of these regulations may result in disciplinary action and that violations of ethics statutes may result in civil and/or criminal penalties.

SUPSHIP should analyze and identify operations with particular potential for misconduct. When warranted, SUPSHIP should develop and execute a plan to minimize that potential misconduct. The following should be considered in formulating such a plan:

- increase surveillance of Government personnel at remote contractor's sites through unscheduled inspections of specific operations by military or civilian supervisors
- reduce tour length of Government personnel at remote sites
- rotate Government personnel among contractor sites
- require that preparation of a specification and inspection or acceptance of work under that specification be performed by different individuals
- audit work authorized on-site for actual completion
- audit accepted work for conformance to specifications
- audit Government Property Administrator's decisions on scrap, repairables, and mandatory returnables
- audit scrap materials sold to contractors by Government property administrators to ensure that materials are scrap
- be alert for signs of affluence not commensurate with the economic status of Government employees
- ensure all SUPSHIP personnel understand the command requirement for absolute adherence to the Standards of Conduct
- be observant for possible falsification of inspection records

2.8 Hotline Policies and Procedures for NAVSEA Shore Activities

[NAVSEAINST 5041.1A](#), reference (i), applicable to all NAVSEA shore activities and detachments, encourages employees to use the chain of command in reporting fraud or relating improprieties. Otherwise, employees are encouraged to use the local Hotline, or NAVSEA, Navy, or DoD Hotlines.

A Hotline may be established at the discretion of the commanding officer. The instruction ensures that Hotline referrals are forwarded to NAVSEA, that complete records and controls are established and maintained, and that examiners are independent, impartial, and free of actual or perceived influence. The instruction gives procedures on publicizing information about Hotline programs and contacting appropriate authorities to respond to fraud or related improprieties.

2.9 Fraud, Waste, and Other Abuse

This section discusses coordination of fraud prevention, indicators of fraud, and actions against fraud.

2.9.1 Coordination for Fraud Prevention

DoD officials are responsible for the integrity of DoD contracts and must be prepared to take immediate action to protect Government integrity and interests when required. Although criminal cases often take years to complete, the DoD can take contractual and administrative actions on less evidence than needed for a criminal conviction. A coordinated approach to criminal, civil, contractual, and administrative actions permits the Government to expedite criminal proceedings. Early action and coordination are essential to ensure that no action taken will adversely affect the Government's ability to pursue any other available action.

The Secretary of Defense (SECDEF) issued [DoDINST 7050.5](#), reference (j), to ensure establishment of a centralized point of coordination. This directive requires that the cognizant criminal investigative organizations inform the centralized points of coordination each time a significant fraud or corruption investigation in procurement or related activities is opened. Through this process, the Government will be able to use its variety of remedies in a more efficient and effective manner. In 2007, SECNAV established the Acquisition Integrity Office (AIO) to manage acquisition fraud matters within DoN. Per [SECNAVINST 5430.92B](#), reference (k), AIO acts as the centralized organization within DoN to monitor and ensure the coordination of all criminal, civil, administrative, and contractual remedies for all cases, including investigations for fraud, waste, and related improprieties related to acquisition activities affecting the DoN. As the centralized organization for acquisition fraud matters, AIO is the single point of contact for all acquisition fraud matters. AIO partners with NCIS and the Naval Audit Service (NAS) to provide investigative support on acquisition fraud cases.

2.9.2 Indicators of Defective Pricing Fraud

Auditors assess pricing situations to determine if the circumstances surrounding any positive defective pricing are indicators of potential fraud. The auditor is responsible for finding and reporting indicators, not proving fraud. The Truth-in-Negotiations Act gives the Government the right to adjust the contract price when the price is based on inaccurate, incomplete, or out-of-date cost or pricing data. Defective pricing occurs when more current, complete, and accurate data exist, but are not provided to the negotiator.

The Defense Contract Audit Agency (DCAA) is responsible for performing reviews of selected contracts and subcontracts. The agency issues a defective pricing report when the auditor finds that the contract price was increased because the contractor did not follow the Truth-in-Negotiations Act. In the past, auditors concentrated on finding defective pricing and not assessing the reason for defective pricing and indications of fraud. The DCAA issued guidance by providing a list of indicators for assessing whether the situation is a sign of possible fraud that should be referred for investigation. The following are indicators of defective pricing fraud that demonstrate the need for further investigation:

- using a vendor other than the proposed vendor
- intentional failure to update cost or pricing data
- selective disclosure
- changed dates
- lost records
- lack of support for proposal
- change in make-versus-buy
- reporting a production break and increased cost when no actual break occurs
- combining items
- intentionally eliminating support to increase the proposal prices
- including inflated rates in the proposal, for example, for insurance or workers' compensation
- intentionally duplicating costs by proposing them as both direct and indirect
- indication of other fraudulent activities which would include material substitution, used or new, and certifying replacement of parts versus repair
- proposing obsolete items that are not needed
- continually failing to provide requested data
- not disclosing an excess material inventory that can be used in later contracts
- refusing to provide data which is requested for elements of proposed costs
- not disclosing actual data from completed work for follow-on contracts
- knowingly using an inter-company division to perform part of the contract but proposing purchase or vice versa
- ignoring established estimating practices
- suppressing studies that do not support the proposed costs
- commingling work orders to hide productivity improvements

- requesting an economic price adjustment clause when the material is already purchased
- submitting fictitious documents
- withholding information on batch purchases
- failing to disclose internal documents on vendor discounts
- failure of prime contractor to pay subcontractor

2.9.3 Actions against Fraudulent Activities

The Government has the right to insist on certain standards of responsibility and business integrity from its contractors and to take a variety of actions against contractors who engage in fraudulent activities. These actions described below are taken in conjunction with, after, or instead of criminal prosecution.

The Civil False Claims Act, [31 USC 3729](#), reference (l), can make a contractor liable for submission of a false claim to the Government and allows the Government to recover damages and penalties for false claims. The Government must suffer monetary damages to recover damages and must prove by a preponderance of evidence that the contractor knowingly submitted a false claim.

The Program Fraud Civil Remedies Act, [31 USC 3801](#) (as amended by [Public Law 110-69](#)), reference (m), allows Federal agencies to impose administrative penalties for certain false claims and statements.

The Contract Disputes Act, [41 USC 601-613](#), reference (n), makes a contractor liable for the amount of any unsupported part of a claim plus the costs of reviewing the claim if it is determined that it is a result of misrepresentation of fact or fraud.

The courts can order the forfeiture of the entire amount of a claim in which it judges the proof is based on contractor fraud or attempted fraud. A contractor risks losing the entire claim even if the claim is only partially based on fraud.

The contracting office has the right to terminate a contract for default because of a contractor's failure to perform. The Government also has the right to terminate a contract for default for other improper conduct, including violation of the Anti-Gratuities Clause ([FAR 52.203-3](#)) and [41 USC 51- 58](#), the Anti-Kickback Act of 1986, reference (o), which prohibits gifts by a subcontractor as inducement for award of the contract.

Rescission is a common law remedy in contracts which allows both parties to return to their position before the contract. This remedy may be used when fraud or corruption occurs in obtaining or awarding the contract. The Government may administratively rescind a contract when there has been a final conviction for bribery, gratuities, or conflicts of interest.

According to [41 USC 605](#), reference (p), contracting officials do not have the authority to pay claims where there is reasonable suspicion of fraud. Contracting officials should not take further action without coordination with the Department of Justice. The provisions of [FAR 9.1](#) state that contracts may only be awarded to responsible contractors. Contractors must affirmatively demonstrate their responsibility, including a satisfactory record of integrity and business ethics.

By provisions of [FAR 9.4](#), contractors may be prohibited from doing business with the Government for the commission of fraud. Suspension is an interim measure; a contractor may be suspended for up to 18 months while the investigation is underway. Debarment is a final determination of a contractor's non-responsibility and may be effective for up to three years. A contracting officer can recommend the debarment of companies and individuals and can impute, in recommending its debarment, the conduct of certain key individuals in that company. Contracting officials must forward reports of improper contractor activity to the suspension and debarment authority at the earliest opportunity to make suspension or debarment effective.

Under [FAR 31.205-47](#), contractors who are found to have engaged in fraud on cost-type contracts are not entitled to recover legal and administrative costs incurred in unsuccessfully defending against Government action.

[10 USC 2408](#), reference (q), provides guidelines on "Prohibition on Persons Convicted of Defense Contract-Related Felonies and Related Criminal Penalty on Defense Contractors". Among other things, the statute bars an individual convicted of fraud or any other felony arising from a contract with the DoD from working in management or a supervisory capacity on any defense contract.

Under [10 USC 2324](#), reference (r), a contractual penalty can be assessed when a contractor submits a claim for a direct or indirect cost when such a cost is specifically ruled unallowable by either statute or regulation. The statute also authorizes a penalty for the knowing submission of defective cost or pricing data.

2.9.4 Government Personnel

The Government has a variety of remedial actions to take against employees who collude with contractors in fraudulent conduct, including: termination, revocation of a contracting officer's warrant, recoupment of lost funds, and administrative penalties for conflicts of interest.

2.10 Managers' Internal Control Program (MICP)

[OMB Circular A-123](#), Management's Responsibility for Internal Control, reference (s), states that "Management is responsible for establishing and maintaining internal controls to achieve the objectives of effective and efficient operations, reliable financial reporting, and compliance with applicable laws and regulations. Management shall consistently apply the internal control standards to meet each of the internal control objectives and to assess

internal control effectiveness.” It requires that commands implement a system of internal controls to provide reasonable assurance that:

1. Programs achieve their intended results
2. Resource use is consistent with the agency mission
3. Programs and resources are protected from waste, fraud, and mismanagement
4. Laws and regulations are followed

[NAVSEAINST 5200.13C](#), Management Control Program (MCP), reference (t), states NAVSEA policy on internal controls and requires that all commands establish Managers’ Internal Control Programs (MICPs) to support commanders and managers in meeting the requirements of OMB Circular A-123. The MICP is a tool to evaluate and report on the effectiveness of internal controls throughout an organization and to identify and, when necessary, take corrective actions to remedy deficiencies. The establishment and verification of internal control effectiveness is essential for leadership to establish reasonable assurance that operational risks are mitigated and internal control deficiencies are promptly identified for corrective action.

The SUPSHIP Managers’ Internal Control Program Manual, Appendix A, mandates establishment of a MICP at each SUPSHIP to support the Supervisor and managers in assessing operational risk, implementing and validating the effectiveness of internal controls, implementing corrective actions as internal control deficiencies are identified, and reporting on the effectiveness of internal controls. It also describes the minimum requirements for MICP execution for consistent application across SUPSHIP offices and to ensure that the Supervisors receive quality and consistent MICP products.

**Appendix 2-A: SUPSHIP Managers' Internal Control
Program (MCIP) Manual**

**Supervisor of
Shipbuilding
Managers' Internal
Control Program (MICP)
Manual**

22 June 2015

Supervisor of Shipbuilding Managers' Internal Control Program (MICP) Manual

Table of Contents

1. Purpose	2-16
2. Scope	2-16
3. Background	2-16
4. MICP Implementation	2-16
5. MICP Plan	2-17
6. Inventory of Assessable Units	2-18
7. Risk Assessment Process	2-19
8. Internal Control Assessment Documentation	2-21
9. Statement of Assurance	2-23
10. Metrics	2-25
11. SUPSHIP MICP Configuration Control Board (CCB)	2-25
Enclosure (1) – Sample AU Inventory	2-27
Enclosure (2) – Sample MICP Risk Assessment Form	2-28
Enclosure (3) – Sample Management Control Review	2-28
Enclosure (4) – Sample Management Control Review Corrective Action Plan	2-29
Enclosure (5) – Sample Statement of Assurance Certification Statement	2-30
Enclosure (6) – New AU Deficiency Form	2-32
Appendix A – SUPSHIP Common and Unique Assessable Units	2-34

References

- (a) OMB Circular A-123, Management’s Responsibility for Internal Control..... 2-16
- (b) NAVSEA 5200.13C, Management Control Program 2-16
- (c) DoDI 5010.4, Managers’ Internal Control Program Procedures..... 2-16
- (d) SECNAV 5200.35, DoN Managers’ Internal Control Program 2-16

Tables

- Table 1 – Levels of Inherent Risk and Control Risk..... 2-21

1. Purpose

This operating manual establishes the mandatory policies, procedures, and responsibilities for the implementation and administration of the Managers' Internal Control Program (MICP).

2. Scope

This manual is effective immediately and is applicable to all Supervisors of Shipbuilding, Conversion, and Repair, USN (SUPSHIPS). All locally issued SUPSHIP instructions establishing a MICP must make reference to this manual as a mandatory use document.

3. Background

a. [OMB Circular A-123](#), Management's Responsibility for Internal Control, reference (a), states that "Management is responsible for establishing and maintaining internal controls to achieve the objectives of effective and efficient operations, reliable financial reporting, and compliance with applicable laws and regulations. Management shall consistently apply the internal control standards to meet each of the internal control objectives and to assess internal control effectiveness." It requires that commands implement a system of internal controls to provide reasonable assurance that:

- 1) Programs achieve their intended results
- 2) Resource use is consistent with the agency mission
- 3) Programs and resources are protected from waste, fraud, and mismanagement
- 4) Laws and regulations are followed

b. Per [NAVSEA 5200.13C, Management Control Program](#), reference (b), it is NAVSEA policy that all commands establish MICPs to support commanders and managers in meeting these responsibilities. The MICP is a tool to evaluate and report on the effectiveness of internal controls throughout their organizations and take corrective actions to remedy deficiencies when necessary. Other tools include, but are not limited to, SUPSHIP Command Evaluation Internal Reviews, external agency audits, and self-assessments. The establishment and verification of internal control effectiveness is essential for leadership to establish reasonable assurance that operational risks are mitigated and internal control deficiencies are promptly identified for corrective action. Further MICP guidance is provided by [DoDI 5010.4, Managers' Internal Control Program Procedures](#), reference (c), and [SECNAV 5200.35, DoN Managers' Internal Control Program](#), reference (d).

4. MICP Implementation

a. Each SUPSHIP shall implement a system of internal controls to provide reasonable assurance that the following objectives are met:

- 1) Effective and efficient operations

- 2) Reliable financial reporting
- 3) Compliance with applicable laws and regulations

b. Each SUPSHIP shall implement an MICP to support commanders and managers in assessing operational risk, identifying internal controls necessary to mitigate these risks, validating the implementation and effectiveness of these internal controls, implementing corrective actions as internal control deficiencies are found, and reporting on the effectiveness of internal controls.

c. Each SUPSHIP MICP shall consist of the following key components:

- 1) MICP Plan
- 2) Inventory of Assessable Units
- 3) Risk Assessment Process
- 4) Internal Control Assessment Documentation
- 5) Annual Statement of Assurance (SOA)
- 6) Program and Performance Metrics

5. MICP Plan

a. The MICP Plan is an executive summary of a command's MICP. The plan captures the organization's approach to implementing an effective internal control program. As required by [SECNAV M-5200.35](#), DoN Managers' Internal Control Manual, the MICP plan shall be updated annually and must identify the following key elements:

- 1) The organization's senior official overseeing the MICP, the MIC coordinator and the alternate MIC coordinator
- 2) An overview of the MICP as related to the GAO standards for internal control
- 3) A description of risk assessment methodology
- 4) A description of monitoring/internal control assessment methodology
- 5) A description of how to develop and track corrective action plans
- 6) MIC training efforts
- 7) The date the plan was last updated

b. An MICP Plan development guide is provided in Example 7 of [SECNAV M-5200.35](#). The guide outlines the key information requirements for each section to provide assistance in developing a robust plan. This format shall be used by each SUPSHIP MIC Program Coordinator to create the organization's plan, which must be updated at least annually.

6. Inventory of Assessable Units

a. [NAVSEAINST 5200.13C](#) requires that each MICP Coordinator establish and maintain an inventory of assessable units (AUs) for the activity's key financial and operational processes, and defines an assessable unit as "Any organizational, functional, programmatic, or other applicable subdivision capable of being evaluated by management control assessment procedures. An assessable unit should be a subdivision of an organization that ensures a reasonable span of management control to allow for adequate analysis." [SECNAV M-5200.35](#) states that "An assessable unit must have clear limits or boundaries and be identifiable to a specific responsible manager. Further, it must be small enough to provide reasonable assurance of adequate management controls but large enough that any detected material weakness has the potential to impact the mission of the organization. Assessable units must constitute the entire organization. This means that every part of the organization must be represented by one of the assessable units in the organization's inventory of assessable units."

b. SUPSHIP MICP Coordinators will collectively develop and maintain an AU Inventory consisting of AU's common to all SUPSHIPS. Each SUPSHIP MICP must include and account for these common AU's and their associated internal controls in their command's MICP. SUPSHIP MICP Coordinators must also maintain a separate AU Inventory of additional AU's that are unique to one or more SUPSHIPS (e.g., SUBSAFE Program). [Appendix A](#) provides a current listing of all SUPSHIP common and unique AUs.

c. AUs must properly reflect the organization and be updated as necessary to reflect changes within the organization and/or its functional managers. At a minimum, the SUPSHIP Common AU inventory must be reviewed semi-annually to ensure its accuracy. Each SUPSHIP command unique AU inventory must be reviewed annually to ensure its accuracy.

d. The SUPSHIP Common AU Inventory and unique AU inventories will contain, at a minimum, the following data:

- AU name
- AU description
- AU risk assessment results
- AU manager name and organization code
- Applicable instruction or guidance documentation
- List of known operational risks
- List of internal controls necessary to mitigate known operational risks

- Reference to management control review or alternative management control review used to validate the implementation and effectiveness of each identified control, as well as the date the effort was performed
 - Identification of corrective actions taken to address identified non-compliances or deficiencies
- e. The template provided in [enclosure \(1\)](#) shall be utilized by each SUPSHIP MIC Coordinator to document the command AU inventory.
- f. The above data fields should be populated through ongoing collaboration between MIC Program Coordinators and AU Managers. MICP Coordinators should meet with AU Managers at least annually to review and update these data fields, including validating that the existing AU Inventory accurately reflects the command's current workload, reviewing and refreshing known risks and internal controls, and identifying ongoing or future efforts which may serve as Alternative Management Control Reviews (AMCRs) as defined in paragraph 8(d) of this manual.

7. Risk Assessment Process

- a. The MICP Risk Assessment process is intended to identify the likelihood and consequence of a process control failure that may impact the organization in meeting its objectives. Designated AU Managers will complete AU Risk Assessments in accordance with paragraph 7(c) and 7(d) of this manual. When assessing the likelihood of process control failures, AU Managers should take into account the adequacy and accuracy of AU process documentation, personnel and budgetary resources available to execute these processes, the extent to which these processes are reviewed, and the adequacy of corrective action procedures for identified deficiencies. When assessing the consequence of process control failures, AU Managers should consider the potential visibility of a control failure, resulting work stoppage issues, impact to personnel or equipment safety, disciplinary actions, and the extent to which the impact of the control failure will be known or contained.
- b. When completing AU risk assessments, AU Managers should also consider uncorrected findings from audits, inspections, or internal reviews and their potential effect or impact on the ability of the command to meet its mission.
- c. AU Risk Assessments should be performed at least once annually. AU Risk Assessments should also be completed in the following circumstances:
- When a new AU Manager is assigned
 - When a new AU is added to the command AU inventory
 - When the AU experiences a significant change in policies and procedures
 - As directed by the commanding officer

d. All SUPSHIP AU Managers will utilize the template in [enclosure \(2\)](#) to perform the AU Risk Assessment. AU Managers or designated Subject Matter Experts (SMEs) should complete the Risk Assessment Form. Risk Assessments performed by someone other than the designated AU Manager must be approved by the designated AU Manager.

e. MICP Coordinators will utilize AU Risk Assessment results to prioritize the MICP effort, including:

- Coordinating identification of AUs that are at high risk for fraud, waste, abuse, and/or mismanagement
- Identifying AU's where management control improvement is required to reduce process control failure likelihood
- Identifying opportunities for a short-notice Management Control Test (see para 8.g)
- Identify AU candidates for inclusion in the Annual Command Evaluation and Review Plan

f. AU Managers, in collaboration with MICP Coordinators, will identify the level of inherent risk and control risk associated with each identified risk and management control within their applicable AU's. The inherent risk and control risk for each identified risk and management control will be subjectively categorized as low, medium, or high. Inherent risk is defined by [SECNAV M-5200.35](#) as the susceptibility to a potential hazard, assuming there are no related specific control activities. Control risk is defined by [SECNAV M-5200.35](#) as the risk that a process failure will not be prevented or detected by the management control. For example, a management control may be designed to prevent or detect the misuse of a government purchase card. The control risk is that the management control will not prevent or detect misuse of a government purchase card. Table 1 below should be used as a guide for determining inherent and control risk levels.

Table 1 – Levels of Inherent Risk and Control Risk

Risk	Low	Moderate	High
Inherent	AU Manager believes the potential risk does not have severe consequences and is unlikely to occur.	AU Manager believes the potential risk has severe consequences or is likely to occur.	AU Manager believes the potential risk has severe consequences and is likely to occur.
Control	AU Manager believes the controls in place will prevent or detect a process control failure.	AU Manager believes controls in place will more likely than not prevent or detect a process control failure.	AU Manager believes the controls in place are unlikely to prevent or detect a process control failure.

8. Internal Control Assessment Documentation

a. In accordance with [SECNAV M-5200.35](#), once internal controls are in place, management shall actively monitor those controls to ensure that they are functioning correctly and effectively mitigating the associated risk. Control assessment documentation can include either Management Control Review (MCR) results or Alternative Management Control Review (AMCR) results.

b. An MCR is a documented evaluation on the effectiveness of an internal control in meeting the control objective.

c. MCRs conducted at SUPSHIPs will be documented using the template provided in [enclosure \(3\)](#) and will include the following information:

- Assessable Unit Name
- Identified Risk
- Management Control in place to mitigate identified risk
- Existing Control Risk Level
 - Low, Medium, High
- Control Objective
 - What is the purpose of the control?
- Control Type
 - Manual or Automated?
- Control Design
 - Detective: Detect undesirable events that have occurred.
 - Corrective: Restore a system to expected state.
 - Preventive: Deter undesirable events from occurring.
 - Directive: Cause desirable event to occur.
 - Separation of Duties: Restrict authority of one person.

- Control Frequency
 - How often is this control function utilized?
- Test Method
 - What actions will be taken to determine the effectiveness of the control?
- Testing Period
 - Timeframe of information under review
- Criteria for Effectiveness
 - What guidelines will be used to determine the effectiveness of the management control under review?
- Test Result Summary
 - Explain Review findings. **If the criteria for effectiveness was not met, note that a corrective action plan is required.**
- New Control Risk Level
 - Low, Medium, High

d. Alternative Management Control Review (AMCR), as defined by [NAVSEAINST 5200.13C](#), is a process developed for other organizational purposes which determines whether or not a management control is operating effectively. Alternative Management Control reviews may include, but are not limited to, the following:

- SUPSHIP Command Evaluation and Review Office Internal Reviews
- Results of audits performed by external agencies including Government Accountability Office, DOD Inspector General, and Naval Audit Service
- NAVSEA Command Compliance Inspections
- Command Investigations
- Internal audits or self-assessments

e. Every assessable unit should be subject to at least one MCR annually, unless all identified management controls are reviewed as a function of an Alternative Management Control Review. An MCR performed by an AU Manager does not need to include all controls each year. The scope of the MCR is based on management's judgment, and should focus first on areas where control risk is identified as medium or high.

f. All identified management controls will be rated as having a low, moderate, or high control risk. Using the results of a MCR or an AMCR, all management control risks should be reclassified. When MCRs or AMCRs find controls to be effective, the reclassified control risk should be classified as medium or low. If the results of a MCR or AMCR find the management control to be ineffective, the control should be reclassified as having a high control risk. In accordance with paragraph 8(i) of this manual, a corrective action plan, found in [enclosure \(4\)](#), should be developed for those controls that are reclassified as having a high control risk.

- g. MICP Coordinators will conduct short-notice MCRs on an ongoing basis. In addition to assessing the command's compliance with applicable regulations and adequacy of internal controls, short-notice MCRs will indicate the command's level of audit readiness. Short-notice Management Control Reviews will also be documented using [enclosure \(3\)](#). A minimum of three short-notice MCRs will be conducted quarterly by each SUPSHIP MICP Coordinator.
- h. All AMCRs and MCRs, whether conducted by the assigned AU Manager or the MIC Program Coordinator, will be identified as a management control validation effort in the Command's AU inventory. To ensure that all internal control validation efforts are properly accounted for, and to avoid any potential duplicity of control validation efforts, all AMCR documentation, including audit reports and self-assessment results, should be provided by the cognizant AU Manager to the MIC Coordinator as it becomes available.
- i. All Management Control Reviews that identify internal control deficiencies require corrective action implementation by the responsible AU Manager. Plans for corrective actions will be documented and approved by the applicable AU Manager using the Corrective Action Plan template in [enclosure \(4\)](#).

9. Statement of Assurance

- a. The Statement of Assurance (SOA) is a command-wide annual report that certifies the commanding officer's level of reasonable assurance as to the overall adequacy and effectiveness of internal controls within the command. The SOA is also used to disclose known management control accomplishments and deficiencies identified using MIC Program processes, and to describe plans and schedules to correct any reported management control deficiencies. The SOA reporting period begins 1 July and ends 30 June.
- b. The submission of the command's SOA will be coordinated by the command MIC Program Coordinator, and developed using the SOA Tool found at: <https://www.fmosystems.navy.mil/soa/login/index.cfm?fuseAction=dspLogin> **
- c. The SOA submission will include the following:
- 1) Cover Memorandum. A cover memorandum signed by the SUPSHIP commanding officer shall provide senior management's assessment as to whether there is reasonable assurance that internal controls are in place and operating effectively. In addition, the SOA must certify to the number of management control reviews that are scheduled for the upcoming MIC year and the number of management control reviews completed during the previous MIC year. The certification must take one of the following three forms:
 - (a) An **unqualified statement of assurance** (reasonable assurance with no material weaknesses reported). Each unqualified statement shall provide a firm

** Denotes secure website requiring NMCI/CAC access

- basis for that position, which the Agency Head (or principal deputy) will summarize in the cover memorandum.
- (b) A **qualified statement of assurance** (reasonable assurance with exception of one or more material weaknesses noted). The cover memorandum must cite the material weaknesses in internal controls that preclude an unqualified statement.
- (c) A **statement of no assurance** (no reasonable assurance because no assessments conducted or the noted material weaknesses are pervasive). The commanding officer shall provide an extensive rationale for this position.
- 2) Accomplishments. This is a brief summary of the most significant accomplishments and actions taken by the command during the SOA reporting period to strengthen internal controls. The accomplishments shall be ordered by significance with the most significant accomplishments listed first. Management control accomplishments may include improved compliance with laws and regulations, improvements in protection of government property, improved efficiency of operations, and increased conservation of command resources.
- 3) Listing of all internal control deficiencies. This will include all uncorrected and corrected Material Weaknesses (MW), Reportable Conditions (RC), and Items to be Revisited (IR). An MW is a management control deficiency, or collection of management control deficiencies, which is significant enough to report to the next higher level. The determination is a management judgment as to whether a weakness is material. An MW impairs or may impair the ability of an organization to fulfill its mission or operational objective. An RC is a control deficiency, or combination of control deficiencies, that adversely affects the ability to meet mission objectives but are not deemed by the Head of the Component as serious enough to report as material weaknesses. An IR is a management control deficiency where insufficient data exists to determine whether the deficiency constitutes an MW or RC.
- 4) Detailed narrative descriptions of all uncorrected MW, RC, and IR including the plans and schedules for corrective actions. This should include those identified during the current year and those disclosed in prior years with updated corrective action information.
- 5) Detailed narrative descriptions of all corrected MWs, RCs, and IRs identified during prior reporting periods.
- d. All AU Managers will provide input to the command SOA by submitting a signed memorandum providing reasonable assurance that the system of internal controls, applicable to their assigned AU's, in place during the current SOA reporting period are adequate and effective. The template to be used by all AU Managers is contained in [enclosure \(5\)](#). Page 2 of enclosure (5) must be completed for all AU's under the cognizance of each AU Manager. Internal Control accomplishments and deficiencies that meet the definition in paragraph 9(C)(2) and 9(c)(3) respectively should be described in detail.

e. MICP Coordinators, through collaboration with AU Managers and the commanding officer, will determine which internal control accomplishments and deficiencies constitute inclusion in the annual SOA submission. MICP Coordinators, using input from AU managers, must complete [enclosure \(6\)](#) for all deficiencies identified in the annual SOA submission.

10. Metrics

a. MICP Coordinators will monitor and document MICP Metrics and MICP Performance Metrics. All metrics will be shared among SUPSHIP community MICP Coordinators on a quarterly basis as described by paragraph 11 (d) of this manual.

b. Program metrics will identify the level to which MICP requirements have been deployed and implemented across each command. At a minimum, each MICP Coordinator will document the following program metrics on a quarterly basis:

- 1) Percentage of AUs in which an AU Manager has been assigned from both the SUPSHIP Common AU Inventory and Unique AU Inventories
- 2) Percentage of AU Managers who have received current MIC Program training
- 3) Percentage of risk assessments performed at the AU level and control level

c. MICP performance metrics will provide information on the effectiveness of the MICP in improving the command's level of compliance with applicable regulations and the command's level of audit readiness. Each MICP Coordinator will document the following performance metrics:

- 1) Compliance Inspection Results. MICP Coordinators will document the total number of non-compliances identified by the NAVSEA Compliance Inspection on a triennial basis.
- 2) MCR Results. On a quarterly basis, MICP Coordinators will develop metrics using the results of MCR's conducted by MICP Coordinators on short notice, and those conducted by AU Managers. This should include the total number of MCRs performed, the percentage of reviews where controls were found to be implemented and effective, and the percentage of reviews where controls were found inadequate and/or ineffective and required corrective action. Metrics for MCRs conducted by the MICP Coordinator should be maintained separately from those conducted by AU managers.

11. SUPSHIP MICP Configuration Control Board (CCB)

a. This manual establishes the SUPSHIP MICP Configuration Control Board (CCB). The MICP CCB will be chaired by NAVSEA 04Z and CCB members will include all SUPSHIP MICP Coordinators. Configuration control is essential to ensuring that policies, procedures, methodologies and forms usage mandated by this manual are not deviated from without prior review and approval by the SUPSHIP MICP CCB.

b. SUPSHIP MICP CCB concurrence and approval is required for the following:

- Deviation from use of standardized documentation

- Modifications to Common AU Inventory
- Modifications to Common Metrics
- Deviation from any other procedures and methodologies mandated by this manual

c. Proposed changes to this manual should be submitted to the SUPSHIP MICP CCB Board and all team members for review, discussion, and approval prior to implementation of any proposed changes. Control of proposed changes is performed under the auspices of SUPSHIP MICP CCB, who will consider all impacts of incorporating the recommended change prior to approval.

d. The SUPSHIP MICP CCB will conduct quarterly teleconferences to discuss MICP changes which require CCB approval as described in paragraph 11(b) of this manual, to discuss common metrics as described in paragraph 10 of this manual, and to address other related SUPSHIP Community MICP matters.

Enclosure (1) – Sample AU Inventory

Managers Internal Control Program - Assessable Unit (AU) Inventory													
CODE	AU MANAGER	ASSESSABLE UNIT NAME	ASSESSABLE UNIT DEFINITION	RISK LEVEL	INSTRUCTION / GUIDANCE	Risks	Mgt Assigned Inherent Risk Level	Mgt Assigned Control Risk Level	Internal Controls	Validation	Date Conducted	New Control Risk Level	Corrective Action Needed?
	POC	MINOR PROPERTY PROGRAM - ADMINISTRATION AND ACCOUNTING PROCESS	Policies and procedures for the custody, accounting and disposition of United States Government property having a unit acquisition cost of \$5,000 or more as well as items that are below \$5,000 and are sensitive, classified, or meet all of the following criteria: (1) pilferable; (2) critical to the activities mission; (3) hard to repair or replace. DPAS Inventory Record Process	L	SUPSHIPGROTINST 7320.2J	Records of property are not created in a timely manner to ensure accountability upon property receipt (not in DPAS in seven days).	Low	Low	In accordance with SUPSHIPGROTINST7320.2K, the PPM will be the designated recipient of all personal property purchases. This will ensure the PPM obtains the property and associated documentation immediately upon receipt and is able to create an accountable record in a timely manner.	CER Review 11-16	1/12/2012	High	Yes, followup tracked via CER standards.
						Physical Property is not adequately marked and cannot be identified as needed to perform inventories.	Low	Low	All items entered into DPAS are required to be tagged as property of the US Government. The assigned serial number will be used to perform inventories as required.	CER Review 11-16	1/12/2012	High	Yes, followup tracked via CER standards.
						Property is not signed out to custodian to assign accountability.	Low	Low	All property must be signed out to a custodian by the PPM, and documentation supporting this is maintained on file.	CER Review 11-16	1/12/2012	High	Yes, followup tracked via CER standards.
						Personal Property spot checks or other routine surveillance is not conducted or conducted without independence, therefore increasing the likelihood that stolen, lost, or misused equipment is not accounted for.	Low	Low	100% floor:book and book:floor inventory completed triennially and supported by documentation identifying who conducted the review and the results of review (to include adjustments made).	CER Review 11-16	1/12/2012	High	Yes, followup tracked via CER standards.
						Personnel are not assigned and designated to serve as Personal Property Managers to ensure implementation, execution, and accountability for Personal Property program requirements.	Low	Low	Letters of designation must be maintained on file to assigned Personal Property Managers.	CER Review 11-16	1/12/2012	Low	No
						Personnel are not assigned and designated to serve as personal property custodians, as needed to ensure that all personal property has an individual assigned to safeguard from theft, loss, or damage.	Low	Low	Letters of designation must be maintained on file to assigned Personal Property Custodians.	CER Review 11-16	1/12/2012	High	Yes, followup tracked via CER standards.

Enclosure (2) – Sample MICP Risk Assessment Form

SUPSHIP MANAGER'S INTERNAL CONTROL PROGRAM RISK ASSESSMENT FORM				
Assesable Unit Title _____				
Risk Assessment Worksheet Part 1: Determine Likelihood of Process Control Failure				
This worksheet helps predict the likelihood of process control failure in five categories of failure causes. For each category, read the table cells and select a whole number which best describes the contribution of that category in predicting failure.				
	Score 1 or 2	Score 2, 3, or 4	Score 4 or 5	Score
Documentation	Process is well documented, controls are usable and understandable.	Process is documented and addresses needed controls, but is not current, complete, is confusing or difficult to understand.	Process is not documented. AU is documented but does not provide needed controls.	
Responsibilities	Most people know their responsibilities are adequately trained, have needed resources to accomplish responsibilities.	Some key people are unclear about their responsibilities or have received training of questionable value. Resources are barely adequate.	Most people do not know their responsibilities are inadequately trained, or do not have needed resources to accomplish responsibilities.	
Internal Reviews	Controls and processes receive frequent review by the process owner.	Some reviews are done, but they are not well understood, and have minimal value.	Controls and processes receive infrequent or no review.	
Non-Compliance	Non-compliance instances have been documented, process exists and is used to find them, compliance exists and is used.	Some non-compliance instances are documented, criteria is used but is not clear; process is not well established.	No non-compliance instances have been documented, no process exists or is used to find them, no compliance criteria exists or is used.	
Corrective Action	Corrective actions have been identified, action has been taken, validation has been performed.	Some corrective actions have been identified, but follow-up is poor or spotty.	Corrective actions have not been identified, action has not been taken, no validation has been performed.	
Likelihood :				#DIV/0!
Risk Assessment Worksheet Part 2: Determine Consequence of Process Control Failure				
This worksheet helps predict the consequence of process control failure by considering five categories of undesirable outcome. For each category, read the table cells and select the rating which best describes the effect of an internal control failure.				
	Score 1 or 2	Score 2, 3, or 4	Score 4 or 5	Score
Visibility	A Division-level (or lower) report of corrective action is likely adequate.	A formal Department- or Division level internal critique is likely.	A formal command-level internal critique, or formal external evaluation is likely.	
Work Stoppage	Process would be briefly stopped or not stopped with little or no cost impact.	Process would be briefly or partially stopped with limited or minor cost impact.	Process would be completely stopped with broad impact.	
Containment	Extent of faulty product or information spill would be known and limited. Costs of containment would be small.	Extent of faulty product or information spill would be moderate or unknown for a short time. Costs of containment would be moderate.	Extent of faulty product or information spill would be broad or unknown for a long time. Costs of containment would be great.	
Discipline	Disciplinary action would be limited to few people, or no disciplinary action.	Disciplinary action would be moderate and limited to few people.	Disciplinary action would be serious. Many people would be disciplined.	
Safety	Few or no people would incur minor injuries only, little or no equipment/plant damage.	Some people would incur minor injuries, some people could incur moderate injuries, some equipment/plant damage.	Some people would incur serious injury, many people would incur moderate injury, serious equipment/plant damage.	
Consequence :				#DIV/0!
Performed By:	_____	_____	_____	
	Print Name	Signature	Date	
Approved By:	_____	_____	_____	
	Print Name	Signature	Date	

Enclosure (3) – Sample Management Control Review

Management Control Review	
Organization:	
Department:	
Preparer:	
Phone:	Email:
Assessable Unit:	DAWIA
Risk:	DAWIA certification is issued to employee's who have not met all certification requirements.
Control:	A two-level DAWIA Certification request review is established. The SUPSHIP Groton DAWIA Coordinator and the Final Approving Authority for the applicable career field review the employee's educational, experience, and DAU training accomplishments prior to approving DAWIA certification requests.
Existing Control Risk Level:	Low
Control Objective:	To ensure that employee issued DAWIA Certification have first completed all educational, experience, and training requirements.
Control Type:	Manual
Control Design:	Detective
Control Frequency:	Continuous
Test Method:	Review DAU Transcripts for all individuals who have received DAWIA certification in the past six months. Ensure that 100% of these employees have completed the required experience, educational, and training requirements.
Testing Period:	Q3 and Q4 FY 2011
Criteria for Effectiveness:	100% of employees sampled must have completed all the required educational, experience, and training requirements prior to approval of DAWIA career field certification request.
Test Result Summary:	
New Control Risk Level:	High
Testing conducted by:	
Name (Print) _____	Signature _____
Results acknowledged by:	
Name (Print) _____	Signature _____

Enclosure (4) – Sample Management Control Review Corrective Action Plan

Management Control Review Corrective Action Plan	
Organization:	
Department:	
Preparer:	
Phone:	Email:
Assessable Unit:	DAWIA
Risk:	DAWIA certification is issued to employee's who have not met all certification requirements.
Control:	A two-level DAWIA Certification request review is established. The SUPSHIP Groton DAWIA Coordinator and the Final Approving Authority for the applicable career field review the employee's educational, experience, and DAU training accomplishments prior to approving DAWIA certification requests.
Existing Control Risk Level:	High
Control Objective:	To ensure that employee issued DAWIA Certification have first completed all educational, experience, and training requirements.
Control Type:	Manual
Control Design:	Detective
Control Frequency:	Continuous
Control Deficiency:	Of the 14 DAWIA Career Field Certifications issued during Q3 and Q4 FY11, only 8 individuals completed the required experience, educational, and training requirements prior to receipt of certification.
Root Cause:	The SUPSHIP Groton DAWIA Coordinator and Final Approving Authorities were not reviewing employee accomplishments prior to approval of career field certification.
Plan for Corrective Action	The SUPSHIP Groton Admin Department Head will provide on the job training for the DAWIA Coordinator and Final Approving Authorities to ensure these individual understand all requirements needed prior to approval of certification requests.
Estimated Completion Date:	Q2 FY12
Approved by:	
Name (Print):	Signature:

Enclosure (5) – Sample Statement of Assurance Certification Statement

30 March 2015

MEMORANDUM

From: AU Manager
To: Code 100
Via: Code 100B

Subj: STATEMENT OF ASSURANCE CERTIFICATION STATEMENT

Encl: (1) Code xxx Assessable Units
(2) New Code xxx Assessable Unit Deficiencies

1. I have reviewed the system of internal controls in effect for the period of 1 April 2014 through 30 March 2015 for Code xxx applicable assessable units identified in enclosure (1). All internal control accomplishments and internal control deficiencies identified between 1 April 2014 and 30 March 2015 are contained in enclosure (1). Plans for corrective action, where applicable, are also contained in enclosure (1).
2. With the exception of any deficiencies identified in enclosures (1) and (2), I have reasonable assurance that internal controls are in place and operating effectively, and that the objectives of the Federal Financial Managers' Integrity Act were achieved.
3. Information to support this certification statement was derived from reviews, audits, inspections, observations, knowledge gained from daily operations of programs, and/or other methods that evaluate internal controls.

J. D. Doe

Assessable Unit Name

ACQUISITION STAFFING (DAWIA) TRAINING PROCESS

Description: The process of providing for all SUPSHIP acquisition training and employee development.

Standards: DON DAWIA Operating Guide

2012-2013 Internal Control Accomplishments

(Explain Accomplishments Below)

2012-2013 Internal Control Deficiencies

(Explain Deficiency Below)

Plans for Corrective Action

(Explain plans to correct above deficiencies)

Enclosure (6) – New AU Deficiency Form

1. Title of Deficiency

2. Description of Deficiency

3. Year Identified

4. Original Targeted Correction Date

5. Current Target Date

6. Validation Process

7. Results Indicator

8. Source(s) Identifying Deficiency

9. Planned Milestones:

a. Current Fiscal Year

b. Next Fiscal Year

Appendix A – SUPSHIP Common and Unique Assessable Units

SUPSHIP Common Assessable Units

PROCUREMENT	
1	Small Purchase Program - Purchase Card Process
CONTRACT ADMINISTRATION	
2	Contract Management - Contract Administration Process
3	Contract Management - Subcontractor Surveillance and Evaluation of Contractor Purchasing Systems
4	Contractor Performance Assessment Rating System (CPARS)
5	Earned Value Management
6	Past Performance Information Retrieval System – Statistical Reporting (PPIRS)
7	Product Data Reporting and Evaluation Program (PDREP)
8	Project Management
9	Quality Assurance (QA) Program
10	Rate Analysis
11	Technical Analysis Review
MANUFACTURING, MAINTENANCE, AND REPAIR	
12	Technical Authority
13	Testing/Certification
PROPERTY MANAGEMENT	
14	Government Property - Program Administration
15	Minor Property Program - Administration and Accounting Process

COMMUNICATIONS / INTELLIGENCE / SECURITY	
16	Telecommunications
17	Security Programs - Information/Industrial Security Process
18	Security Programs - Communications Security Process
19	Security Programs - Continuity of Operations Planning (COOP)
20	Security Programs - Force Protection and Physical Security Process
21	Security Programs - Operational Security Process
22	Security Programs - Personnel Security Process
23	Security Programs - Courier Program Administration
INFORMATION TECHNOLOGY	
24	Information Technology - Hardware/Software Management Program
25	Information Technology - Information Assurance Program
26	Information Technology - Network Management
PERSONNEL AND/OR ORGANIZATION MANAGEMENT	
27	Employee Development Program - Acquisition Staffing (DAWIA) Training Process
28	Employee Development Program - Personnel Management Process
29	Military Programs

COMPTROLLER AND/OR RESOURCE MANAGEMENT	
30	Financial Management Program - Official Travel Program
31	Financial Management Program - Civilian Payroll Process (Timekeeping)

32	Financial Management Program - Certification of Invoices
33	Financial Management (General)
	SUPPORT SERVICES
34	Administrative Support Program - Records Management
35	Command Evaluation and Review Program - Audit Liaison and Follow-Up Process
36	Command Evaluation and Review Program - Hotline Reporting Process
37	Command Evaluation and Review Program - Internal Review Process
38	Freedom of Information
39	Managers' Internal Control Program (MICP) - Administration Process
40	Privacy Act Protection Process
41	Safety Program - Environmental Safety and Health Process
42	Standards of Conduct Process
	OTHER (PRIMARILY TRANSPORTATION)
43	Government Vehicle Administration

SUPSHIP Unique Assessable Units

	SUPSHIP BATH
1	Small Business Program
2	Dry Dock Operations
3	Logistics Support Management
4	Classified Hardware Control
5	Military SAPR

6	Military Command Managed Equal Opportunity
7	Military Physical Readiness Program
8	Military Urinalysis Program
9	Military MWR
10	Transportation Incentive Program (TIP)
11	Tech Authority

SUPSHIP GROTON	
1	SUBSAFE/Deep Submergence/Fly-by-Wire Ship Control System Programs
2	Administrative Support Program – Message Usage and Handling Process
3	Civilian Employee Training and Career Development
4	Employee Development Program – Award Process
5	Information Technology Program – Support Services Process
6	Technical Support Management (TSM) System
7	Policy and Procedures Relating to Follow-Up on Contract Audit Reports
8	Transportation Incentive Program (TIP)

SUPSHIP GULF COAST	
1	Records Management
2	Asset Management
3	Military Personnel Programs

	SUPSHIP NEWPORT NEWS
1	Service Contracting
2	Undefinitized Contract Actions
3	Asset Management
4	Information Technology (IT) Security Implementation
5	Personally Identifiable Information (PII) - Information Assurance
6	Sexual Assault
7	Employees Activity Association
8	Morale, Welfare, and Recreation (MWR) Program
9	Transportation Incentive Program (TIP)
10	Policy and Procedures Relating to Follow-Up Contract Audit Reports
11	SUBSAFE/Deep Submergence/Fly-By-Wire Ship Control System Program
12	Civilian Employee Training and Career Development
13	Legal Review and Assistance

Appendix 2-B: Acronyms

ACO	Administrative Contracting Officer
AIO	Acquisition Integrity Office
AMCR	Alternative Management Control Review
AU	Assessable Unit
CCB	Configuration Control Board
CFR	Code Of Federal Regulations
DAEO	Designated Agency Ethics Official
DCAA	Defense Contract Audit Agency
DoD	Department of Defense
DoDD	Department of Defense Directive
DoN	Department of the Navy
FAR	Federal Acquisition Regulations
HCA	Head of the Contracting Activity
IR	Item to be Revisited
MCR	Management Control Review
MICP	Managers' Internal Control Program
MW	Material Weakness
NAS	Naval Audit Service
NAVSEA	Naval Sea Systems Command
NAVSEAINST	Naval Sea Systems Command Instruction
NCIS	Naval Criminal Investigative Service
OMB	Office of Management and Budget
PCO	Procuring Contracting Officer

PL	Public Law
RC	Reportable Condition
SOA	Statement of Assurance
SECDEF	Secretary of Defense
SECNAVINST	Secretary of Navy Instruction
SSA	Source Selection Authority
SSEB	Source Selection Evaluation Board
USC	United States Code