DEPARTMENT OF THE NAVY
BUREAU OF MEDICINE AND SURGERY
7700 ARLINGTON BOULEVARD
FALLS CHURCH VA 22042

BUMEDINST 5200.13C
BUMED-N81
19 Mar 2025

BUMED INSTRUCTION 5200.13C

From: Chief, Bureau of Medicine and Surgery

Subj: INTEGRATED RISK MANAGEMENT PROGRAM

Ref: (a) Federal Managers' Financial Integrity Act of 1982
(b) GAO-14-704G Standards for Internal Control in the Federal Government (Green Book) of September 2014
(c) GAO-15-593SP, Framework for Managing Fraud Risks in Federal Programs of July 2015
(d) OMB Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control of July 2016
(e) DoD Instruction 5010.40 of 11 December 2024
(f) Department of Navy Enterprise Risk Management Framework of May 2024
(g) DON FY 2025 Integrated Risk Management Implementation Handbook of 11 October 2024
(h) OPNAVINST 5200.25F
(i) OPNAVINST 5450.215F
(j) Navy Medicine Campaign Plan 2028

Encl: (1) Acronyms
(2) Definitions
(3) Risk Assessment Guidance - Internal Controls Over Reporting – Operations
(4) Components of Effective Internal Control Accomplishment or Deficiency Write-up
(5) IRM Coordinator Appointment Letter Template
(6) Assessable Unit Manager Appointment Letter Template
(7) Assessable Unit Representative Appointment Letter Template
(8) Generic Assessable Unit Questionnaire - Internal Controls Over Reporting – Operations
(9) Waiver for Alternate Signature Template

1. Purpose. To provide policy and assign responsibilities for the Bureau of Medicine and Surgery (BUMED) Integrated Risk Management (IRM) Program. To support a commitment to integrity, ethical values, competence, and accountability in performance by providing updated guidance to BUMED commands for implementing an effective IRM Program. This instruction is a complete revision and should be reviewed in its entirety.

2. Cancellation. BUMEDINST 5200.13B.

3. Scope and Applicability. This instruction applies to all Navy Medicine commands and activities.

4. Background

a. References. References (a) through (h) establish the IRM Program throughout the Department of the Navy (DON) per Federal regulations and standards. The terminology, standards, and other applicable concepts used in this instruction are provided in enclosure (1).

b. Internal Controls. Internal controls are the tools managers use to ensure compliance with laws, regulations, and policies; promote operational economy and efficiency; safeguard resources against fraud, waste, abuse, and misuse; and ensure the data represented in significant reports driving management decisions are accurate and reliable. Internal controls apply to all programs, functions, and organizational elements. Internal controls are sound management practices used to support the effectiveness and integrity of all processes and provide continual feedback to management for controlling risk.

c. Reviews. The implementation and execution of BUMED's IRM Program is subject to compliance reviews in conjunction with DON inspections and audits.

5. IRM Organizational Structure

a. Reference (h) provides a visual representation of the IRM alignment, detailing scope, risk response examples and lead organizations for each of its components.

b. BUMED's IRM Instruction incorporates reporting requirements from the DON. References (g) and (h) guide reporting from BUMED to DON. BUMED must report to the office of primary responsibility for the following components respectively:

(1) Enterprise Risk Management (ERM). ERM provides an enterprise-wide lens to risks enhancing the quality, validity, and reliability of mission-critical decision-making. Per reference (h), Deputy Under Secretary of the Navy (DUSN) Management (M) Performance Improvement Office (PIO) is the office of primary responsibility for ERM and is responsible for the execution and reporting of the DON ERM activities. Director, Navy Staff Internal Control Office (DNS-F5) is the ERM point of contact for the Chief of Naval Operations (CNO). Assessing and prioritizing risks is an important step in operationalizing the strategic plan through the development of program plans, budgets, and establishment of performance goals and controls.

(2) Operations-Internal Controls Over Reporting (ICOR-O). ICOR-O includes the plans, methods, policies and procedures to conduct non-financial operations and ensure accurate recording and reporting of non-financial information. It provides structure for program managers to monitor program, operational, and administrative internal controls over all non-

financial processes and Information Technology (IT) within BUMED. ICOR-O objectives are met through functional area or program assessments, deficiency identification, root cause analysis, and corrective action implementation. Per reference (h), CNO is the office of primary responsibility for the DON ICOR-O activities and reporting.

(3) ICOR – Financial (ICOR-F). ICOR-F provides structure for program managers to monitor internal controls over all financial processes and IT within BUMED. Per reference (h), ICOR-F includes both financial reporting (ICOR-FR) and financial systems (ICOR-FS). ICOR-F ensures and provides reasonable assurance on financial information being complete, accurate, and reliable; and reported in compliance with applicable laws and regulations. ICOR-F objectives are met through internal control assessments, deficiency identification, root cause analysis, and corrective action implementation. Per reference (h), Office of the Assistant Secretary of the Navy (OASN) Financial Management and Comptroller (FM&C) is the office of primary responsibility for the DON ICOR-F activities and reporting.

6. Policy Implementation

a. Surgeon General of the Navy. It is the policy of the Surgeon General of the Navy, who also performs the duties of Chief, BUMED, to implement an effective IRM Program and appoint an Enterprise IRM Program Coordinator and Alternate IRM Program Coordinator(s). These appointees are responsible for the administration and coordination of the IRM Program to align with the reporting requirements established in reference (a) through (j). Each echelon is required to establish a formal IRM Program and is responsible for assessing risk and establishing internal controls throughout their organization that include the five standards outlined in reference (b): control environment, risk assessment, control activities, information and communications, and monitoring.

b. Implementation. Implementation of this program should not duplicate existing control efforts, but rather complement other efforts (e.g., Financial Improvement and Audit Readiness Program, Naval Safety Program, Operational Risk Management Program, BUMED Inspector General Program, external audits, inspections, etc.). BUMED will publish fiscal year IRM Program Guidance annually that will guide BUMED commands' IRM efforts for that program year. The fiscal year IRM Program Guidance will identify assessable units (AU) to be reviewed for the ICOR-O, ICOR-FR, and ICOR-FS components of IRM. The guidance will outline the sampling and testing methodology that will be used to meet the requirements of reference (d), appendices A and D. Additionally, the guidance will detail quarterly and annual IRM reporting requirements and other specific instructions.

7. Roles and Responsibilities

a. Surgeon General of the Navy

(1) Must establish a positive control environment by involving managers at all levels throughout the organization and advocate accountability for establishing, evaluating, and improving controls within each AU.

(2) Must identify and appoint in writing a full-time Enterprise IRM Coordinator and an Alternate IRM Coordinator responsible for overseeing the IRM Program as the Enterprise IRM Coordinator, per reference (h). The Enterprise IRM Coordinator and Alternate IRM Coordinator must be a government civilian or active-duty military member. The Enterprise IRM Coordinator and Alternate IRM Coordinator positions cannot be assigned as a collateral duty, and the responsibilities must be part of the position description (PD) (civilian) or formal job duties (active duty).

(3) Must establish an independent IRM team or office, led by the Enterprise IRM Coordinator, that has direct access to the Executive Office. This team and office must not be located within the Inspector General or Comptroller's Offices.

(4) Must appoint in writing BUMED Assessable Unit Managers (AUMs), who must be government personnel (civilian or active duty) assigned to a leadership position that serves as the end-to-end (E2E) process-level manager for their AUs (also referred to as DON Business Process Areas), per reference (g). The appointees are responsible for assisting the BUMED IRM Coordinator with administering the IRM Program to align with the reporting requirements in reference (a).

(5) Must establish a command instruction for the Enterprise IRM Program and review annually for revisions.

(6) Must oversee the performance of risk assessments within BUMED.

(7) Must sign the IRM command instruction and the fiscal year (FY) statement of assurance (SOA) package. The annual SOA package is comprised of the BUMED integrated certification statement memorandum, the consolidated IRM risk assessment template, the internal control evaluation (ICE) report, and corrective action plans (CAPs). The SOA package must be submitted to the DNS-F5 by the due dates established annually by DNS-F5. BUMED must report any data collected after the reporting date in the next reporting cycle. In the event Surgeon General of the Navy is unable to sign the SOA package, a waiver must be request with justification to DNS-F5 using enclosure (8).

b. Echelon 3, 4 and 5 Commanders, Commanding Officers, and Officers in Charge

(1) Must establish and maintain a positive control environment across his or her area of responsibility (AOR) and advocate accountability for establishing, evaluating, and improving controls within each applicable AU.

(2) Require managers at all levels and across all functional areas to establish, evaluate, and improve internal controls.

(3) Must identify and appoint in writing an IRM Coordinator, per reference (h). When possible, commands should also appoint an Alternate IRM Coordinator. Commands should consider the size of the command and the IRM workload to determine if the command IRM Coordinator should be full-time or part-time. The IRM Coordinator and Alternate IRM Coordinator position cannot be assigned as a collateral duty, meaning the duties must be included in the PD (civilian) or formal job duties (active duty). In the absence of an incumbent, the IRM Coordinator at the echelon 4 level must be assigned responsibility for echelon 5 IRM activities.

(4) Must establish an independent IRM team or office, led by the IRM Coordinator, that has direct access to the executive office, per reference (h). The IRM team and office must not be located within the Inspector General or Comptroller's Offices. Recommended command structure is in the strategic planning, process improvement or similar command functions, however the exact location of the IRM function should be determined by the commander, commanding officer, or officer in charge.

(5) Must oversee the performance of risk assessments within their organization.

(6) Must report all material weakness and significant deficiency control findings to the echelon above the reporting command.

(7) Must submit the signed Quarterly IRM Certification Statements providing levels of assurance with ICOR-O, ICOR-FR, and ICOR-FS. ICOR-O reporting is required for all BUMED commands regardless of source funding per references (a) through (h). ICOR-FR and ICOR-FS reporting is required for all commands receiving TI-17 funding.

(8) Echelon 3 and 4 commands must submit the signed command Statement of Assurance Letter and CAPs (as applicable) to the BUMED IRM Coordinator by the suspense date in the fiscal year BUMED IRM Program Guidance. Commands must report any data collected after the report date in the next reporting cycle. Echelon 5 commands should coordinate with the echelon 4 IRM Coordinator to determine SOA requirements.

(9) Must appoint in writing AUMs. AUMs must be government civilian or active-duty Service member assigned to leadership positions that serve as the E2E process-level managers

appointees are responsible for assisting the command IRM Coordinator with administering the for their AUs. The IRM Program to align with the reporting requirement in reference (a). AUMs must be appointed by the commander, commanding officer, or officer in charge unless the IRM Coordinator has been delegated appointment authority.

c. BUMED IRM Coordinator and Alternate Enterprise IRM Coordinator(s) (Echelon 2)

(1) Must administer, coordinate, and ensure BUMED IRM Program compliance with references (a) through (h) and this instruction.

(2) Must issue fiscal year IRM Program Guidance annually to the BUMED HQ activity and echelon 3 commands for further distribution to the required BUMED IRM reporting commands. The fiscal year IRM Program Guidance details the internal BUMED reporting deadlines and internal control risk categories to be assessed based on the DON and CNO's instruction and higher tasking.

(3) Identify and document all AUs within BUMED. The AUs must be documented in the annual AUM appointment letter. AUs selected for testing will be documented in the annual BUMED IRM Guidance.

(4) Coordinate with the AUMs to identify and appoint in writing Assessable Unit Representatives (AUR). AURs must be active duty Service members or civilian employees serving in leadership positions serving as the process-level managers for their assessable units. AURs may be appointed by the BUMED IRM Coordinator or the AUM.

(5) Coordinate with AUMs, AURs or subject matter experts (SME) at the Enterprise level to conduct risk assessments and develop AU internal control assessments. Provide AUMs and SMEs with AU internal control assessment results. As necessary, assist AUMs and/or SMEs with the development of CAPs in response to internal and external internal control assessment and audit findings.

(6) Provide AU assessment templates, populated with applicable information to support ICOR-O, ICOR-FR, and ICOR-FS efforts, to the BUMED HQ activity and echelon 3 IRM Coordinators for further distribution to subordinate commands that are identified as BUMED IRM reporting entities per the fiscal year IRM Program Guidance.

(7) Complete applicable IRM Program Trainings per reference (h).

(8) Apprise organization and subordinate commands of IRM Program training opportunities. Track IRM Program training for subordinate commands and IRM Coordinators and Alternate Coordinators for subordinate commands via an annual data call to the BUMED HQ Activity and echelon 3 IRM Coordinators.

(9) Provide detailed implementation instruction, templates, and training on the concept objectives, policies, responsibilities, and procedures for the IRM Program to BUMED HQ activity and the echelon 3 command IRM Coordinators for further distribution to subordinate commands.

(10) Prepare the annual BUMED SOA package during the reporting period as defined by CNO guidance. Submit the SOA package, accompanied by supporting components, that includes BUMED's level of assurance that ICOR-O, ICOR- FR, and ICOR-FS are operating effectively for signature by Surgeon General of the Navy and Chief, BUMED.

(11) Follow-up on all BUMED IRM Program material weaknesses reported via the SOA package and evaluate actions taken by management to correct these deficiencies.

(12) Collaborate with command leadership to establish BUMED risk appetite and tolerance levels.

d. IRM Coordinator and Alternate IRM Coordinator (BUMED Reporting Entities (BUMED HQ Activity, Echelon 3, and Echelon 4))

Please Note: Per annual BUMED IRM Program guidance, echelons 3 and 4 are designated IRM Reporting Entities and are responsible for internal control oversight at subordinate commands. They may designate subordinate commands as reporting entities responsible for the formal program requirements indicated in this section. This distinction does not change the requirement to appoint IRM Coordinators at all command levels.

(1) Must administer, coordinate, and ensure BUMED IRM Program compliance with references (a) through (h) and this instruction.

(2) Echelon 3 commands may develop and disseminate program guidance and reporting requirements, if needed to supplement the annual fiscal year IRM Guidance issued by the BUMED IRM Coordinator.

(3) Must coordinate with the AUMs to identify and appoint in writing AURs. AURs must be active-duty Service members or civilian employees assigned to leadership positions serving as the process-level managers for their assessable units. AURs may be appointed by the command IRM Coordinator or the AUM.

(4) Must annually, in coordination with the BUMED IRM Coordinator, identify mandatory and elective AUs to be assessed. All IRM reporting entities will identify their ICOR-O elective AU topics per the fiscal year IRM Program Guidance.

(5) Must conduct risk assessments with AUMs or SMEs.

(6) Must work with AUMs to develop AU internal control assessments for any program areas identified as high risk due to absence or ineffectiveness of internal controls. Enclosure (8) may be used as a guide for developing an ICOR-O AU assessment.

(7) Must review quarterly ICOR-O, ICOR-FR, and ICOR-FS AU assessment results (as applicable) for the reporting command and subordinate commands (as applicable) for completeness, ensuring assessments follow the guidance and standards set by the BUMED IRM Coordinator. If errors, omissions, or misrepresentations of information are found, assessments must be returned for correction, completion, or explanation.

(8) Must assist AU program managers with the development and implementation of CAPs where ineffective, weak, or nonexistent internal controls are identified. Ensure CAPs include targeted resolution dates and monitor CAP implementation to ensure deficiencies are fully corrected or reported to higher echelon when higher level assistance is needed. Where CAPs span multiple activities within the reporting entity, coordinate planning and implementation of improvement efforts.

(9) Must prepare the command's quarterly IRM certification statements and annual SOA in conformance with the BUMED fiscal year IRM Program Guidance, based on:

(a) Reviews of mandatory ICOR-O, ICOR-FR, and ICOR-FS AUs.

(b) Reviews of elective AUs.

(c) Other sources of internal control data identified (i.e. financial statement audit, Department of Defense, DON, medical inspector general (MEDIG) inspection findings, external audits such as Naval Audit Service (NAVAUDSVC) and Government Accountability Office (GAO), etc.).

(10) Must brief quarterly IRM Certification Statements and the annual SOA to the commander, commanding officer, or officer in charge. Topics addressed should include, but not be limited to, ICOR-O, ICOR-FR, and ICOR-FS AU results; new internal control deficiencies and CAPs; and CAP implementation for existing internal control deficiencies.

(11) Must maintain documentation for higher-level reviews and audit purposes.

(12) Must complete the required trainings as instructed by the BUMED IRM Coordinator. BUMED HQ Activity and echelon 3 IRM Coordinators are required to maintain a list of subordinate commands IRM Coordinators and Alternate Coordinators and track IRM Program training for the IRM coordinators and alternate coordinators within their AOR. BUMED HQ Activity and echelon 3 IRM Coordinators must respond to the BUMED IRM Coordinator's annual training data call.

(13) Must use informed judgment to determine the materiality of all identified control deficiencies. References (b) and (j) define the different categories of control deficiencies and criteria for materiality. If required to submit an annual SOA per the BUMED fiscal year IRM Program Guidance, maintain thorough documentation to support a decision to exclude any auditor or IG-identified material weaknesses from the organization's annual SOA.

(14) Must assign a senior accountable official responsible for developing and overseeing execution of a CAP for each material weakness reported. The senior accountable official must be a senior DON official at the flag officer or senior executive service level. If the command does not have an official at that rank or grade, the commander, commanding officer, or officer in charge will be the senior accountable official and will not further delegate this responsibility. Commands must follow corrective action plan requirements as outlined in reference (h) for identified significant deficiencies and material weaknesses.

e. BUMED N-Codes (Echelon 2). Must support CAP implementation and collaborate with the BUMED IRM Coordinator to issue new or revised policies that will bring internal controls within specific programs, financial areas, or systems into compliance with established laws and regulations.

8. Records Management

a. Records created as a result of this instruction, regardless of format or media, must be maintained and dispositioned per the records disposition schedules located on the DON Assistant for Administration, Directives and Records Management Division portal page at https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/DRM/Records-and-Information-Management/Approved%20Record%20Schedules/Forms/AllItems.aspx

b. For questions concerning the management of records related to this instruction or the records disposition schedules, please contact the local records manager or the OPNAV Records Management Program (DNS-16).

9. Review and Effective Date. Per OPNAVINST 5215.17A, BUMED-N81 will review this instruction annually around the anniversary of the issuance date to ensure applicability, currency, and consistency with Federal, Department of Defense, Secretary of the Navy, and Navy policy and statutory authority using OPNAV 5215/40, Review of Instruction. This instruction will be in effect for 10 years, unless revised or cancelled in the interim and will be reissued by the 10-year anniversary date if it is still required, unless it meets one of the exceptions in OPNAVINST 5215.17A, paragraph 9. Otherwise, if the instruction is no longer required, it will be processed for cancellation as soon as the need for cancellation is known following guidance in OPNAV Manual 5215.1 of May 2016.

10. Information Control Management. Reports required in this instruction are exempt from reports control per Secretary of the Navy Manual 5214.1 of December 2005, part IV, subparagraph 7k.

D. K. VIA

Releasability and distribution:
This instruction is cleared for public release and is available electronically only via the Navy Medicine Web site, https://www.med.navy.mil/Directives/

ACRONYMS

AOR	Area of Responsibility
AU	Assessable Unit
AUM	Assessable Unit Manager
AUR	Assessable Unit Representative
BUMED	Bureau of Medicine and Surgery
CAP	Corrective Action Plan
CNO	Chief of Naval Operations
CUEC	Complementary User Entity Control
DHA	Defense Health Agency
DNS-F5	Director, Navy Staff, Internal Control Program Office
DON	Department of the Navy
DUSN	Department Under Secretary of the Navy
ERM	Enterprise Risk Management
FISCAM	Federal Information System Controls Audit Manual
FY	Fiscal Year
GAO	Government Accountability Office
IC	Internal Control
ICE	Internal Control Evaluation
ICOR-F	Internal Controls Over Reporting - Financial
ICOR-FR	Internal Controls Over Reporting - Financial Reporting
ICOR-FS	Internal Controls Over Reporting - Financial Systems
ICOR-O	Operations -Internal Controls Over Reporting
IG	Inspector General
IT	Information Technology
IRM	Integrated Risk Management
MEDIG	Medical Inspector General
NAVAUDSVC	Naval Audit Service
OASN FM&C	Office of the Assistant Secretary of the Navy – Financial Management & Comptroller
PD	Position Description
PEO	Program Executive Office
PIO	Performance Improvement Office
RMIC	Risk Management Internal Control
SME	Subject Matter Expert
SOA	Statement of Assurance
SOP	Standard Operating Procedure

DEFINITIONS

1. AU. A programmatic or functional area capable of being evaluated by internal control assessment procedures. An AU also may refer to a DON business process area. AUs are identified based upon the programs, processes, administrative activities, or functions significant to mission accomplishment. The AU should be small enough to provide reasonable assurance of adequate internal controls and large enough to detect any material weaknesses that would have a potential impact on BUMED's mission. BUMED publishes annual fiscal year guidance identifying the AUs each required IRM reporting entity will review for the fiscal year. Heads of commands and managers may use local risk assessments to develop elective AUs, as a supplement to mandatory AUs.

2. AUM. The AUM must be a military member or government employee appointed in writing assigned to a leadership position that serves as the process-level manager for their assessable unit(s). AUMs must be appointed by their commander, commanding officer, officer in charge or IRM coordinator if delegated appointment authority. AUMs support the IRM coordinators in fulfilling the IRM program requirements.

3. Complimentary User Entity Controls (CUEC). Internal controls that a system user is responsible for implementing and overseeing to ensure transactions are properly authorized and executed prior to transmission to an external service organization. System owners may assign CUECs to the system user at the entity level.

4. Control Activities. Ensures management directives are carried out. They are the policies, procedures, techniques, and mechanisms that enforce management's directives and provide reasonable assurance that actions are taken to address risks. Control activities are an integral part of an entity's planning, implementing, reviewing, and accountability for stewardship of government resources and achieving effective results. Examples of control activities are top-level review of actual performance; reconciliation of actual and recorded inventory; access restrictions to classified information; and segregation of duties. (This is one of the five standards for internal control prescribed by the GAO in reference (f).)

5. Control Deficiency (CD). A control deficiency exists when the design, implementation, or operation of a control does not allow management or personnel, in the normal course of performing their assigned functions, to achieve control objectives and address related risks. CDs are the least severe of the materiality levels. CDs can often be remediated internally with minimal interruption to the entire organization or need for notification to the next level up in the command by a specific group or sub-group.

6. Control Environment. Leadership and personnel should establish and maintain an environment throughout the organization that sets a positive and supportive attitude toward

internal control and conscientious management. It provides discipline and structure as well as the climate that influences the quality of internal control. (This is one of the five standards for internal control prescribed by the GAO in reference (f)).

7. CAP. A written document that describes the specific steps necessary to resolve a control deficiency, including targeted milestones, completion dates, and accountable parties responsible for implementing the milestones. Milestones should be:

a. Specific. Define the scope of the problem, avoid being broad and describe clear actions that will be taken to fix the deficiency.

b. Measurable. Identify and quantify completion criteria and results for each milestone.

c. Achievable. Corrective actions should be within the reporting organization’s capacity and its existing resources to implement. It must be noted in the CAP if the reporting organization depends on another organization to act.

d. Realistic. Corrective actions should be within the reporting organization’s existing resources to complete. Corrective actions requiring new resources must be included in future budget requests.

e. Time-bound. Time milestones so they may be implemented properly and within realistic expectations.

8. Federal Information System Controls Audit Manual (FISCAM). The FISCAM provides a methodology for performing effective and efficient information system controls audits, either alone or as part of a performance audit, a financial audit, or an attestation engagement, including communication of any identified control weaknesses. FISCAM is consistent with National Institute of Standards and Technology’s guidelines for complying with the Federal Information Security Modernization Act of 2014.

9. Information and Communication. The quality information management and personnel communicate and use to support the internal control system.

10. Internal Controls. A process effected by an entity’s oversight body, management, and other personnel that provides reasonable assurance that the objectives of an entity are achieved. Internal controls are plans, policies, methods, procedures, and other mechanisms in place to mitigate risks and ensure an organization, function, program, or activity’s mission is achieved while also combating against fraud, waste, abuse, and misuse of resources. Internal controls are designed to be detective or preventive in nature.

11. ICOR. Internal controls that provide reasonable assurance over the reliability of reporting for internal and external use and decision-making.

a. ICOR-O. Includes program, operational and administrative controls with the exception of controls over financial reporting. ICOR-O is also inclusive of non-financial IT systems. Operational controls are meant to effectively manage and safeguard an organization's operations. They facilitate mission achievement, such as combat readiness, by ensuring activities are conducted efficiently and effectively. Operational controls are broad and often operate in tandem with and compliment financial, and system controls. Examples of operational controls include (but are not limited to) activities related to personnel (e.g., training), ethics (e.g., fraternization), or safety (e.g., physical security).

b. ICOR-FR. Includes financial reporting internal controls. Financial controls are implemented to prevent fraud, waste, and financial misstatement. Financial controls mitigate the abuse of resources and support the integrity and accuracy of financial statements and financial reporting. They facilitate the achievement of an organization's financial goals and ensure compliance with Federal, regulatory, and statutory fiduciary obligations and requirements. For example, the DoD is required by congressional mandate to undergo an annual financial statement audit, whereby all DoD components are required to support achievement of this requirement and ensure financial statement accuracy. The evaluation of and reporting on financial controls is required under the Federal Managers' Financial Integrity Act of 1982 and Federal Managers' Financial Integrity Act of 1996.

c. ICOR-FS. Includes financial management systems internal controls and conformance with Federal requirements. System controls (FM & Non-FM), or IT security controls, are used by, or are performed by, IT systems to support management of risk, inclusive of policies, procedures, guidelines, practices, or organizational structures which can be of an administrative technical, management, or legal nature, as described by National Institute of Standards and Technology. These controls aim to provide reasonable assurance that the IT system used by an organization operates as intended, its data is reliable, and the organization complies with applicable laws and regulations. These system controls can be further aligned to one of two major categories based on FISCAM.

12. Levels of Assurance

a. Unmodified. Reasonable assurance that internal controls are effective with no material weaknesses reported. Certification must be accompanied by a firm basis for this position.

b. Modified. Reasonable assurance that internal controls are effective with the exception of one or more material weaknesses. Certification must cite material weaknesses that precluded an unmodified statement.

c. No Assurance. No reasonable assurance that ICs are effective because few or no assessments were conducted, the noted material weaknesses are pervasive across many key operations.

13. Materiality. The threshold above which a deficiency or error could prevent the organization from accomplishing mission objectives or reporting reliable financial data for management to use in the decision-making process. Some factors to consider when determining the appropriate severity level of the deficiency or error are the following: impact on mission success or failure; health and safety; threat to image; pervasiveness throughout the organization; or management's reliance on the financial data impacted. The level of materiality becomes more significant as a deficiency or error has a greater impact on those factors.

14. Material Weakness

a. ICOR-O: A material weakness or combination of significant deficiencies, that adversely affects the DON's ability to initiate, authorize, record, process, or report operational (non-financial) data reliably. These deficiencies have a high probability of resulting in significantly degraded DON business process operations performance including efficiency and effectiveness aspects.

b. ICOR-F: Material weakness, or combination of significant deficiencies, that adversely affects the DON's ability to initiate, authorize, record, process, or report financial data reliably. These deficiencies have a high probability of resulting in significantly degraded DON business process operations performance to include efficiency and effectiveness aspects.

15. Monitoring. Activities management establishes and operates to assess the quality of performance over time and promptly resolve the findings of audits and other reviews.

16. Reasonable Assurance. An informed management judgment regarding the overall adequacy and effectiveness of ICs to deter or detect material failures based upon available information that the systems of ICs are operating per reference (a) objectives. There is a high degree of confidence but not absolute confidence.

17. Risk. The possibility an event will occur and adversely affect the achievement of objectives. Risk assessment is the identification and analysis of risks related to achieving the defined objectives to form a basis for designing risk responses.

18. Root Cause Analysis. A focused analysis of a deficiency or exception to determine why it occurred and what action needs to be taken to correct it.

19. Significant Deficiency. A significant deficiency, or combination of control deficiencies, that in management's judgement, represents significant deficiency in the design or operation of internal controls that could adversely affect the DON's ability to meet its internal control objectives.

a. ICOR-O: These deficiencies are more-than-remotely likely to cause a more-than-inconsequential error in significant operational (non-financial) reports that will not be detected or prevented.

b. ICOR-F: These deficiencies are more-than-remotely likely to cause a more-than-inconsequential error in significant financial reports that will neither be detected nor prevented.

20. Senior Accountable Official. A DON manager at the flag officer or senior executive service level who is appointed, in writing, to oversee prompt resolution of a material weakness a command identifies in its annual SOA.

21. Risk Assessment. Senior leadership engagement is necessary to establish and promote a risk conscious organization. Enterprise risk management will influence decision making at the enterprise level, as well as internal control activities throughout the organization. Additionally, managers at all levels of the organization should regularly conduct risk assessments within their areas of responsibility (AOR). Such assessments help identify areas where the absence of effective internal controls poses the greatest risk to mission accomplishment. Managers should consider risks to overall operations, accurate and reliable financial reporting, and compliance with laws and regulations. Questions listed in subparagraphs 21a through 21g may help identify the greatest risks within programs:

a. What could go wrong in the process?

b. What processes require the most judgment?

c. What processes are most complex?

d. What must go right for proper reporting?

e. How could we fail to report accurately?

f. How do we know whether we are achieving our objectives?

g. What business areas are most vulnerable to fraud, waste, and abuse?

Please Note: When conducting a risk assessment, managers should consider the likelihood and impact of a hazard or misstatement, the likelihood an internal control would detect or prevent a hazard or misstatement, as well as the potential materiality of the hazard or misstatement. Enclosure (3) provides guidance on how to conduct a risk assessment for ICOR-O program areas or AUs.

22. Quarterly Certification Statements. The quarterly certification statements will cover the ICOR-O, ICOR-FR, and ICOR-FS (as applicable) assessments conducted during the quarter

and document the command's level of assurance over ICOR-O, ICOR-FR, and ICOR-FS (as applicable). The specific due dates will be provided in the annual fiscal year IRM guidance.

23. SOA. The annual SOA will cover a time period outlined in the annual fiscal year IRM guidance. All BUMED reporting entities required by the annual fiscal year IRM guidance to submit an annual SOA will include internal controls reviewed during the fourth quarter of the prior fiscal year, as well as, internal controls reviewed during the first three quarters of the current fiscal year. If a deficiency is identified after the SOA is signed, but before the reporting period closes, and if it remains an uncorrected deficiency, it should be included in the next year's SOA. The specific due date will be provided in the annual fiscal year IRM guidance.

a. Include management's separate assertion (unmodified, modified, or no assurance) for each component of IRM (i.e., ICOR-O, ICOR-FR, and ICOR-FS (as applicable)) assessed during the reporting timeframe.

b. Document sources of internal control data used to determine the levels of assurance. Only those sources that were used should be listed. The sources may include but are not limited to: ICOR-O AU assessments; external audits (e.g., financial statement examination or audit notices of findings and recommendations, NAVAUDSVC, GAO, Joint Commission, etc.); DoD, DON, MEDIG inspection reports; site assist visits; informal testing; program reviews (e.g., Procurement Performance and Management Assessment Program, logistics assist visits, etc.); and management observation.

c. Include management's assessment of the extent to which all applicable BUMED standard operating procedures (SOP) are employed. Management will explain the basis for the assessment, including, but not limited to, audit preparation testing and site assist activities.

d. Be signed by the head of the command, unless specified otherwise in the annual fiscal year IRM guidance.

e. Identify all ineffective internal controls, as appropriate, as well as CAPs with targeted resolution dates to remediate the ineffective internal controls. Ineffective internal controls must be properly documented per the requirements outlined in the annual fiscal year IRM guidance. Supporting documentation for the annual SOA may include: accomplishment write-ups, deficiency write-ups, CAPs, a compilation of internal control assessment data from sources other than IRM, and SOP compliance.

RISK ASSESSMENT GUIDANCE
INTERNAL CONTROLS OVER REPORTING – OPERATIONS

1. Reference (e) requires that a risk assessment be included as part of an agency's Risk Management Program (IRM is the DON Risk Management Program) process for assessing ICOR-O, ICOR-FR and ICOR-FS. This enclosure will focus on risk assessment guidance for ICOR-O, however, many of the principles may also be applied to ICOR-FR and ICOR-FS.

2. A risk assessment helps identify potential hazards or unwanted actions that might prevent the AU from achieving its objectives. AUMs are best able to conduct risk assessments on their programs due to their expert knowledge of the program's objectives and challenges. In addition to their program experience and oversight, AUMs should consider information from IG inspections, external audits, and Anti-Fraud Program Risk Assessment to help identify additional risks. It is recommended that AUMs work with their command's IRM coordinator to complete the risk assessment.

3. According to reference (d), "management should identify internal and external risks that may prevent the organization from meeting its objectives." AUMs should consider the risks associated with the objective of the AU. Consider the questions in subparagraphs 3a to 3f to help identify risks:

a. What is the objective of the AU?

b. What could go wrong that would prevent the AU from meeting its objective?

c. Where are our vulnerable areas?

d. What processes require the most judgment or are the most complex?

e. What must go right for us to meet the objective?

f. How do we know whether we are achieving our objectives?

4. All BUMED IRM reporting entities are required to complete the risk assessment section of the ICOR-O AU questionnaire. AUMs must identify three risks that, regardless of likelihood or impact, could prevent the functional area from meeting its identified objectives. The risk assessment includes:

a. Risk. A risk is a potential hazard or unwanted action that might prevent the AU from achieving its objective. Consider risks that are internal to the command (e.g., training, downsizing, managerial responsibilities, etc.) and also risks that are external to the command (e.g., changing technology, new regulations, risk associated with contractors, etc.).

b. Mitigating Internal Control. An internal control is a process, policy, procedure, or component of a command's structure used by management to help a command achieve its objectives and reduce or prevent risk. Internal controls help a command run its operations efficiently and effectively, report reliable information about its operations, and comply with applicable laws and regulations. For each risk identified, list all internal controls that have been implemented to mitigate that risk. You may list multiple mitigating internal control for each risk. Internal controls may be detective in nature (designed to identify that an undesired outcome has occurred) or preventative in nature (designed to stop an undesired outcome from occurring). A periodic reconciliation of a supply inventory against orders and historic usage is an example of a detective control. Locking supplies in a cabinet is an example of a preventative control.

c. Likelihood - [High, Medium, or Low] – Think about the likelihood that the risk will occur in an environment where no internal controls are in place. Based on the likelihood that the risk will occur, assign High, Medium, or Low, following the descriptions provided in the Table 1-1:

Likelihood	Description
Low	The risk is unlikely to occur.
Medium	The risk is somewhat likely to occur.
High	The risk is more likely than not to occur.

Table 1-1

d. Impact - [High, Medium, or Low] – Identify the impact the risk would have on the objective if it occurred. Based on the impact that the risk would have on the objective if it were to occur, assign High, Medium, or Low, following the descriptions provided in the Table 1-2:

Impact	Description
Low	The risk will not substantively impede the achievement of the objective.
Medium	The risk will cause some elements of the objective to be delayed or not be achieved.
High	The risk will cause the objective to not be achieved.

Table 1-2

e. Control Risk - [High, Medium, or Low] – This is the risk that the internal control will not mitigate against the identified risk as intended. This is a measurement of the perceived effectiveness of the internal control. The Table 1-3 provides a brief description of the three levels of control risk:

Control Risk	Description
Low	Controls will prevent or detect any hazard or aggregate misstatements that could occur.
Medium	Controls will more likely than not prevent or detect any hazard or aggregate misstatements that could occur.
High	Controls are unlikely to prevent or detect any hazard or aggregate misstatements that could occur.

Table 1-3

Example 1: Pharmacy employees taking office supplies home for personal use is identified as a potential risk. The likelihood is assessed as "high" while the impact is assessed as "low." Due to the low dollar value of office supplies purchased and management not having time to monitor how every pencil and paper clip is used, the only control in place is an annual review of the total amount spent on office supplies. The control risk is "medium."

Example 2: Pharmacy employees taking narcotics home for personal use is identified as a potential risk. The likelihood is assessed as "medium" while the impact is assessed as "high." The pharmacy conducts a weekly physical inventory of all narcotics and reconciles that inventory against filled prescriptions and manufacturer turn-ins and assigns that control a control risk of "low."

COMPONENTS OF EFFECTIVE INTERNAL CONTROL ACCOMPLISHMENT OR DEFICIENCY WRITE-UP

1. Ensure all accomplishments and deficiencies are internal control related. Accomplishments reported in the annual SOA may include: program enhancements to the IRM program, actions taken within programs that enhanced internal controls, or control deficiencies that were identified and corrected during the fiscal year reporting period.

2. Report all accomplishments and deficiencies from your organization's perspective. If a subordinate command reports a deficiency to you, do not simply forward it up the reporting chain. Consider whether that deficiency is really a deficiency for your organization. If it is, describe the deficiency and report it accordingly. If it is not, do not report it, but internally monitor resolution of the deficiency.

3. Consolidate accomplishments and deficiencies reported by subordinate commands if it makes sense to do so. If three subordinate commands each report an identical deficiency related to an AU, consider reporting all three as a single deficiency for your organization. Again, internally monitor resolution of the deficiency at all three subordinate commands.

4. Be succinct.

5. Provide enough detail so that the accomplishment or deficiency gets sufficient higher-level attention. If you report a deficiency that requires higher-level assistance, you need to provide enough detail so that the scope of the issue and the importance of resolving it is clear.

6. If you need higher-level assistance resolving a deficiency, ask for help when you write it up in the quarterly certification statement or annual SOA. What do you need assistance with and from whom?

7. Write up the accomplishment or deficiency so that someone who isn't a subject matter expert will understand. Avoid unnecessary use of technical jargon. Some of the people who read our SOA may have a limited understanding of BUMED. They may not use the automated systems we are talking about. They may not be financial experts. If you don't describe an accomplishment in terms that someone can understand, it won't be appreciated.

8. Spell out acronyms the first time they are used in each accomplishment or deficiency.

9. Make sure any corrective action dates reported for deficiencies are accurate. If the targeted corrective action date has already passed by the time you prepare the quarterly certification statement or annual SOA, no one will know whether the weakness was resolved, or the preparer made an error.

10. Quantify results whenever possible. What is the potential financial impact if the deficiency is not fixed? What percentage of our inventory is unaccounted for? How many man hours did we save annually through an accomplishment?

INTEGRATED RISK MANAGEMENT COORDINATOR
APPOINTMENT LETTER TEMPLATE
(command letterhead)

5200
Ser [Code]/[serial number]

From: Commander, Activity Name
To: [Name of IRM Coordinator (Primary)]

Subj: APPOINTMENT AS INTEGRATED RISK MANAGEMENT PROGRAM COORDINATOR

Ref: (a) OPNAVINST 5200.25F
(b) BUMEDINST 5200.13C
(c) BUMED Fiscal Year Integrated Risk Management Program Guidance

1. Per reference (a) through (c), each BUMED command must appoint an organizational Integrated Risk Management (IRM) Program Coordinator and IRM Program Alternate Coordinator. These appointees are responsible for the administration and coordination of the IRM Program to align with the reporting requirements outlined in reference (a).

2. Effective immediately, you are appointed as the IRM Coordinator for [command name]. This responsibility includes oversight of IRM efforts throughout [command name]. You will be guided in the performance of your duties by the provisions of references (a) through (c).

3. As the [command name] IRM Coordinator, you will facilitate the implementation of an effective governance process to establish and maintain compliance with noted policy and Navy Medicine guidance. Your responsibilities as described in references (a) through (c) will include:

a. Reporting requirements:

(1) Support IRM oversight and the establishment of governance to ensure that [command name] is adhering to all policies and procedures.

(2) Analyze, compile, and coordinate signature of the quarterly IRM certification statements and the fiscal year Statement of Assurance Package for [command name] before submitting to your higher-level echelon command.

(3) Appoint Assessable Unit Managers if delegated the authority.

b. Process improvement:

(1) Identify best business practices and recommend to [command name] leadership ways to improve control documentation, enhance controls, eliminate inefficient controls, and/or implement new controls.

(2) Ensure identified efficiencies, "best practices," and deficiencies are shared within [command name].

c. Review assessments:

(1) Assist [command name] in:

(a) Establishing risk management practices to identify and manage risks related to mission-support and other operations as determined by management.

(b) Identifying internal control objectives based on risk assessment.

(c) Performing self-assessments of organizations and core business lines; identifying deficiencies; and developing and tracking corrective action plans, including milestones to correct deficiencies.

(2) Maintain documentation that will assist in the completion of IRM requirements such as operational process flows, narratives, and associated risk matrices or lists; control objectives; control activities; testing results; and certification statements.

d. Perform audit reviews for operations, financial reporting, and financial systems (as applicable):

(1) Obtain and review findings and recommendations of internal and external audits.

(2) Identify control deficiencies through audit review, communicate the review results with [command name] senior leadership, and document for submission to the BUMED IRM Program Office and other stakeholders as required.

e. Liaise with the next higher echelon IRM Coordinator for Internal Control Over Reporting deficiencies related to operational, financial, and systems processes (as applicable):

(1) Communicate with the next higher echelon IRM Coordinator any deficiencies identified through internal assessments that may impact [command name]'s level of assurance over its internal control environment or a BUMED-level deficiency or strategic initiative.

(2) Monitor and track corrective action plan implementation for any [command name] deficiencies (i.e. material weakness or significant deficiency) listed in the [command name] Statement of Assurance.

4. The appointment is valid until rescinded.

[commander or commanding officer signature block]

ACKNOWLEDGEMENT

By my signature, I acknowledge my appointment as [command name] IRM Coordinator. I have read and understand my responsibilities, accountability, and duties as described in the appointment letter and references (a) through (c). I further understand and acknowledge that this appointment will remain in effect until revoked in writing, or until I am transferred, separated for any reason, or retired from federal service.

____
[Name]
Primary

Please Note:

1. Organizations must use this template to appoint an Assessable Unit Manager (AUM). Letters must be submitted to your higher-level echelon command.
2. Text that is in brackets ([ ]) should be replaced by the preparer
3. Please delete these notes before signing the appointment letter.

ASSESSABLE UNIT MANAGER APPOINTMENT LETTER TEMPLATE

[DD MMM YY]

MEMORANDUM

From: [Commander, Commanding Officer, Officer in Charge)
To: [Group or Name of Assessable Unit Manager]

Subj: APPOINTMENT AS ASSESSABLE UNIT MANAGER

Ref: (a) Integrated Risk Management Coordinator Appointment Letter
(b) OPNAVINST 5200.25F
(c) Navy Medicine Fiscal Year Integrated Risk Management Program Guidance

Encl: (1) [Command Name] List of Assessable Units and Appointments of Assessable Unit Managers

1. Per references (a) through (c), each Navy Medicine echelons 3, 4, and 5 commands is required to appoint a military or government civilian Assessable Unit Manager (AUM) for all Assessable Units (AU) within the command. The [name of your command] commander or commanding officer or IRM Coordinator (if delegated appointment authority) may appoint the AUM. These appointees are responsible for assisting the IRM Coordinator with administering the integrated risk management program to align with the reporting requirements of the Federal Managers' Financial Integrity Act (FMFIA).

2. Effective immediately, you are appointed as an AUM for [name of business] [process or assessable unit] within the name of your command. This responsibility includes successfully managing the IRM program throughout name of business [process or assessable unit]. You will be guided in the performance of your duties by the provisions of reference (b) and (c).

3. As a [name of business process or assessable unit] AUM, you will support the IRM Coordinator to establish and maintain compliance with noted policy and reference (b). Some of your responsibilities will include the following as described in references (b) and (c):

a. Communicate regularly with the IRM coordinator.

b. Assess risks and deficiencies that may adversely affect the organization's mission or operations.

c. Review processes and procedures to provide recommendations for the enhancement, elimination, or implementation of assessable unit internal controls.

d. Communicate regularly with the IRM Coordinator.

Subj: APPOINTMENT AS ASSESSABLE UNIT MANAGER

e. Assess risks and deficiencies that may adversely affect the organization's mission or operations.

f. Review processes and procedures to provide recommendations for the enhancement, elimination, or implementation of assessable unit internal controls.

g. Document operational, administrative, system, and financial internal controls and business processes.

h. Test the effectiveness of the internal controls.

i. Develop corrective action plans.

j. Track progress of corrective action plans.

k. Maintain documentation in a central location to give to the IRM Coordinator as requested that will assist in the completion of IRM requirements such operational process flows, narratives, and associated risk matrices or lists; control objectives; control activities; testing results; and certification statements.

l. Appoint and be supported by one or more Assessable Unit Representative (AUR).

4. The appointment is valid until rescinded in writing, either through a separate memo or removal of the individual's name from enclosure (1) during the annual review process conducted by the IRM Coordinator.

[printed name or signature block of signer]

Please Note:
1. Organizations must use this template to appoint an Assessable Unit Manager (AUM). Letters must be submitted to your higher level Echelon Command.

2. Text that is in brackets ([ ]) should be replaced by the preparer with non-italicized black font.

3. Please delete these notes before signing the appointment letter.

[Command Name] List of Assessable Units and
Appointments of Assessable Unit Managers

Business Process (Assessable Unit)	Appointed Assessable Unit Manager

ASSESSABLE UNIT REPRESENTATIVE APPOINTMENT LETTER TEMPLATE

[DD Mmm YYYY]

MEMORANDUM

From: [(IRM Coordinator or Assessable Unit Manager]
To: [Name of Assessable Unit Representative]

Subj: APPOINTMENT AS ASSESSABLE UNIT REPRESENTATIVE

Ref: (a) Assessable Unit Manager Appointment Letter
(b) OPNAVINST 5200.25F
(c) Navy Medicine Fiscal Year Integrated Risk Management Program Guidance

1. Per references (a) through (c), each Navy Medicine echelon 3, 4 and 5 command Integrated Risk Management (IRM) Coordinators or Assessable Unit Managers (AUM) may appoint an Assessable Unit Representative (AUR). The appointees are responsible for assisting the AUM in their duties that align with the Bureau of Medicine and Surgery IRM Program to align with the reporting requirements of the Federal Managers' Financial Integrity Act (FMFIA).

2. Effective immediately, you are appointed as an AUR for [name of business process or assessable unit] within the [name of your command]. You will be guided in the performance of your duties by the provisions of reference (b) and (c).

3. As a [name of business process or assessable unit] AUR, you will support the AUM to establish and maintain compliance with noted policy and reference (b) and (c). Some of your responsibilities will include in subparagraphs 3a through 3f as described in references (b) and (c):

a. Assess risks that may adversely affect the organization's mission and operations.

b. Review processes and procedures to provide recommendations for the enhancement, elimination, or implementation of assessable unit internal controls.

c. Test the effectiveness of the internal controls.

d. Develop corrective action plans.

e. Track progress of corrective action plans.

f. Maintain documentation in a central location to give to the IRM Coordinator as requested that will assist in the completion of IRM requirements such operational process flows, narratives, Subj: APPOINTMENT AS ASSESSABLE UNIT REPRESENTATIVE

and associated risk matrices or lists; control objectives; control activities; testing results; and certification statements;

4. The appointment is valid until rescinded in writing, by the AUM or IRM Coordinator.

[printed name or signature block of signer]

Please Note:

1. Organizations must use this template to appoint an Assessable Unit Representative (AUR). AURs may be appointed by the Command IRM Coordinator or the AU's Assessable Unit Manager (AUM)

2. Text that is in brackets ([ ]) should be replaced by the preparer with non-italicized black font.

3. Please delete these notes before signing the appointment letter.

GENERIC ASSESSABLE UNIT QUESTIONNAIRE
INTERNAL CONTROLS OVER REPORTING – OPERATIONS

1. The BUMED fiscal year IRM Program Guidance will specify requirements for elective AUs for the BUMED IRM Reporting Entities. However, commands may develop their own AUs outside of the IRM requirement. The AUs should be mission-specific. Use the questions listed as an example when developing assessment questions:

a. Does the command have a current SOP or instruction for the program?

b. Is there a monitoring system in place to assess compliance with applicable SOP/or instructions? If yes, describe the monitoring system.

c. Are there accurate position descriptions on file for each program staff position?

d. Are program staff responsibilities adequately defined and understood?

e. Are education and training resources adequate to provide program staff with the appropriate level of training?

f. Are personnel properly assigned according to their level of training and experience?

g. If required, are personnel properly appointed to their program management position?

h. Do personnel have access to all referenced materials?

i. What are the strengths of the program?

j. What are the program problems or weaknesses?

k. What are the inherent risks in the program?

l. Is there a mechanism for identifying areas of potential misuse?

m. What preventive, detective, and corrective controls are in place to ensure compliance and efficiency, and prevent fraud, waste, and abuse?

n. Is separation of duties in place for inherently high-risk transactions or functions?

o. How often are surveys conducted?

p. Are random checks conducted to monitor compliance?

q. Are there routine inspections or exercises to ensure personnel have knowledge regarding specified situations?

r. How often are internal reviews conducted?

s. Have there been any external reviews or audits completed in this area? When? By whom (e.g., GAO, Navy IG, Naval Criminal Investigative Service, NAVAUDSVC, etc.)? What were the findings?

t. Does the command have performance metrics to monitor the success of the program?

u. Is a plan coordinated with local and civilian agencies?

v. Are there backup deployment systems in place in case of emergencies?

WAIVER FOR ALTERNATE SIGNATURE TEMPLATE

[DD Mmm YY]

MEMORANDUM

From: [Commander or Senior Leader]
To: [DNS-F Representative]

Subj: REQUEST FOR WAIVER TO DELEGATE SIGNATURE AUTHORITY

Ref: (a) OPNAVINST 5200.25F
(c) SECNAVINST 5200.35G

1. Per reference (a), if ([name of commanding officer] is unable to sign the Integrated Risk Management certification statements, a request for waiver to delegate signature authority must be submitted with justification to Director, Navy Staff Internal Control Office (DNS-F5).

2. [Justification provided on this line].

[Printed name or signature block of signer]

Please Note:

1. Organizations must use this template to request for waiver to delegate signature authority

2. Text that is in brackets ([ ]) should be replaced by the preparer with non-italicized black font.

3. Please delete these notes before signing the appointment letter.