U.S. Department of Homeland Security
United States Coast Guard

Commandant
United States Coast Guard

2703 Martin Luther King Jr. Ave SE
Washington, DC 20593-7000
Staff Symbol: VCG
Phone: 202-372-4100

COMDTNOTE 5200
10 JUN 2020

CANCELLED:
09 JUN 2022

COMMANDANT NOTICE 5200

Subj: COAST GUARD ENTERPRISE RISK MANAGEMENT AND ANNUAL STATEMENT OF ASSURANCE REPORTING REQUIREMENTS

Ref: (a) Office of Management and Budget (OMB) Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control (rev. Jul 2016)
(b) Office of Management and Budget (OMB) Circular No. A-11, Preparation, Submission, and Execution of the Budget (rev. June 2019)
(c) DHS SOPDDS Memo "Financial Audit and Enterprise Risk Management (ERM) Approach", dtd 29 Apr 2019
(d) Executive Management Council – Audit, Risk, and Compliance (EMC-ARC) Charter
(e) GPRA Modernization Act of 2010 (GPRAMA), 124 Stat. 3866 (P.L. 111-352)
(f) Federal Managers' Financial Integrity Act (FMFIA) of 1982, 31 U.S.C. § 3512, (P.L. 97-255)
(g) Government Accountability Office (GAO) 14-704G, Standards for Internal Control in the Federal Government (the "Green Book")
(h) Department of Homeland Security Financial Accountability Act (DHS FAA) of 2004, 31 U.S.C. §3516 (P.L. 108-330)
(i) Reports Consolidation Act of 2000, 31 U.S.C. §3516 (P.L. 106-531)
(j) Chief Financial Officers Council (CFOC) and Performance Improvement Council (PIC), Playbook: Enterprise Risk Management for the U.S. Federal Government (rev. Jul 2016)
(k) Management's Responsibility for Internal Control, COMDTINST 5200.10 (series)
(l) Commandant's Guiding Principles 2018-2022

1. PURPOSE. To identify Assessable Organizational Elements (AOE) and establish requirements that these AOEs report to the Commandant the level of assurance of the effectiveness of their internal control over operations, reporting, and compliance in accordance with Reference (a), and to establish

DISTRIBUTION – SDL No.170

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A																										
B	*	X	X		X	X	X	X	X		X	X		X		X	X	X		X	X	X	X		X	X
C			X								X															
D	X				X																					
E					X		X		X														X			
F																										
G																										
H				X		X		X		X	X															

NON-STANDARD DISTRIBUTION: Ba;(CG-092), (CG-094), (CG-1), (CG-11), (CG-12), (CG-13), (CG-2), (CG-4), (CG-5P), (CG-5R), (CG-7), (CG-8), (CG-9), (CG-LGL), (CG-R), (CGCC), DCO-I, DCO, DCMS

guidelines for risk reporting in alignment with References (a) through (d). This Commandant Notice supports compliance with OMB and DHS requirements that risk management and internal control be integrated, risk profiles developed in coordination with annual strategic reviews, and risks taken into account when assessing control effectiveness.

2. ACTION. The following are identified as Senior AOEs and Subordinate AOEs, which will comply with the provisions of this Commandant Notice.

   a. Senior AOEs are: Commander, Coast Guard Atlantic Area (LANT-00); Commander, Coast Guard Pacific Area (PAC-00); Deputy Commandant for Mission Support (DCMS); Deputy Commandant for Operations (DCO); Director of Governmental & Public Affairs (CG-092); Judge Advocate General & Chief Counsel (CG-094); and Assistant Commandant for Resources/Chief Financial Officer (CG-8).

   b. Subordinate AOEs are: Assistant Commandant for Human Resources (CG-1); Director of Health & Safety (CG-11); Director of Civilian Human Resources, Diversity & Leadership (CG-12); Commander, Personnel Service Center (PSC); Superintendent, Coast Guard Academy (CGA); Assistant Commandant for Intelligence (CG-2); Assistant Commandant for Engineering & Logistics (CG-4); Assistant Commandant for Prevention Policy (CG-5P); Assistant Commandant for Response Policy (CG-5R); Assistant Commandant for Command, Control, Communications, Computers & Information Technology/Chief Information Officer (CG-6); Assistant Commandant for Capability (CG-7); Assistant Commandant for Acquisition/Chief Acquisition Officer (CG-9); Senior Procurement Executive & Head of Contracting Activity (CG-91); Commander, CGCYBER Command (CGCC); Assistant Commandant for Reserve (CG-R); Director of International Affairs & Foreign Policy (DCO-I); Director of Operational Logistics (DOL); and Commander, Force Readiness Command (FORCECOM).

   c. Internet release is authorized.

3. DIRECTIVES AFFECTED. COMDTNOTE 5200 dated 8 Apr 2019 is hereby cancelled.

4. BACKGROUND. The Secretary of the DHS is required to provide the President and Congress an annual assurance statement on the state of the Department's internal controls. While the assurance statement is included as part of the Agency Financial Report (AFR), the required assurances are not solely financial. The Department is further required to: implement ERM; continuously build risk identification capabilities into the framework to identify new or emerging risks, and/or changes in existing risks; and integrate risk management and internal control functions. Operational risks must be considered when providing assurance that internal controls are meeting organizational objectives. The Department's Chief Financial Officer (CFO) coordinates the process to support the Secretary's annual assurance statement; however, managing risk and ensuring and reporting on proper internal controls to support the DHS mission is a responsibility of all Component Heads, Departmental lines-of-business, and federal managers.

   a. The Department requires each DHS Component Head to submit to the Secretary an annual assurance statement on the state of their internal controls. DHS components are also tasked with continuing to develop, implement, and mature ERM efforts which manage risks to missions,

goals, and objectives to the Component, including maintaining and updating Component-level Operational and Enterprise Risk Registers. Components should consult their Risk Registers and ERM activities to inform their management assurances. The Commandant's Statement of Assurance (SOA) to the Department is submitted annually and must include specific assurances regarding the Coast Guard's ERM and internal control programs.

b. While assurances provided by AOEs may only concentrate on a segment of the internal control requirements, it is important for all participants in the internal control program to have an understanding of how the assurances they provide over the internal controls within their respective programs influence the Coast Guard's overall assurance statement. Among the assurances provided by the Commandant with respect to the Coast Guard's internal controls are the following:

(1) FMFIA, Section 2, (commonly referred to as Section 2 of the Integrity Act), requires the Commandant's SOA to assert or deny reasonable assurance that Coast Guard controls are achieving their intended objectives, and to report on any existing material weaknesses in the controls. Exceptions to assurance are those that satisfy one or more of the following criteria:

(a) Merits the attention of the Executive Office of the President and the relevant Congressional oversight committees;

(b) Violates statutory or regulatory requirements;

(c) Impairs fulfillment of essential operations or missions;

(d) Deprives the public of needed services.

(2) Section 4 (c) for DHS FAA requires assertion of internal controls that apply to financial reporting by DHS, including considerations of fraudulent reporting. Testing and evaluation results of Coast Guard internal controls over financial reporting (ICOFR) are a primary factor in providing Section 4 (c) assurance.

(3) Section 4 of FMFIA requires the SOA to indicate that financial management systems conform to government-wide requirements. If they do not substantially conform, the statement must list the nonconformities and discuss plans for bringing them into substantial compliance. Information technology general controls (ITGC) testing results reported by Commandant (CG-6) are a large factor in the reported assurance in this Section.

(4) The Reports Consolidation Act of 2000 requires assessment of the completeness and reliability of performance and financial data used in the Department's AFR. Any material inadequacies in the completeness and reliability of the data, and actions being taken to resolve such inadequacies, must be described.

(5) OMB Circular No. A-123 requires agencies to implement an ERM capability coordinated with the strategic planning and strategic review processes established by GPRAMA, and the internal control processes required by FMFIA and the "Green Book".

(6) Appendix A of OMB Circular No. A-123 provides a methodology for management to assess, document and report on internal controls over reporting (ICOR). Further, it integrates ICOR with ERM processes and reasonable assurances over internal controls. The goal of this change is to strengthen financial stewardship and accountability to meet management needs, provide transparency, reduce the reporting burden and provide management with the flexibility to determine the manner in which the annual assurance over ICOR is achieved.

c. While this Commandant Notice outlines an annual reporting requirement, frequent data-driven reviews are identified in OMB Circular A-11 as a best practice. References (a) and (j) expand on this by charging that ERM should not be an isolated exercise, but instead, should be integrated into the management of the organization and eventually into its culture.

5. DISCLAIMER. This guidance is not a substitute for applicable legal requirements, nor is it itself a rule. It is intended to provide operational guidance for Coast Guard personnel and is not intended to, nor does it impose, legally-binding requirements on any party outside the Coast Guard.

6. MAJOR CHANGES. This Note has been updated to align with DHS and OMB guidance reflecting an increased role of ERM within the federal government. Additionally, content has been reorganized from previous versions of this Note to streamline messaging and reduce redundancy.

7. ENVIRONMENTAL ASPECT AND IMPACT CONSIDERATIONS.

a. The development of this Notice and the general policies contained within it have been thoroughly reviewed by the originating office in conjunction with the Office of Environmental Management, Commandant (CG-47). This Notice is categorically excluded under current Department of Homeland Security (DHS) categorical exclusion (CATEX) A3 from further environmental analysis in accordance with Implementation of the National Environmental Policy Act (NEPA), DHS Instruction Manual 023-01-001-01 (series).

b. This Notice will not have any of the following: significant cumulative impacts on the human environment; substantial controversy or substantial change to existing environmental conditions; or inconsistencies with any Federal, State, or local laws or administrative determinations relating to the environment. All future specific actions resulting from the general policy in this Notice must be individually evaluated for compliance with the National Environmental Policy Act (NEPA), Department of Homeland Security (DHS) and Coast Guard NEPA policy, and compliance with all other applicable environmental mandates.

8. DISTRIBUTION. No paper distribution will be made of this Commandant Notice. An electronic version will be located on the following Commandant (CG-612) web sites. Internet: https://www.dcms.uscg.mil/directives/, and CGPortal: https://cg.portal.uscg.mil/library/directives/SitePages/Home.aspx.

9. PROCEDURE. Related procedures and supplemental guidance can be found in the SOA Process Guide on the Commandant (CG-85) CGPortal Page: https://cgportal2.uscg.mil/units/cg85/SitePages/Home.aspx.

10. RECORDS MANAGEMENT CONSIDERATIONS. This Commandant Notice has been evaluated for potential records management impacts. The development of this Commandant Notice has been thoroughly reviewed during the Directives clearance process, and it has been determined there are no further records scheduling requirements in accordance with Federal Records Act, 44 U.S.C. 3101 et seq., National Archives and Records Administration requirements, and the Information and Life Cycle Management Manual, COMDTINST M5212.12 (series). This policy does not make any significant or substantial change to existing records management requirements.

11. DISCUSSION. This Commandant Notice provides ERM and Internal Control reporting guidance, and specific deliverables for completing required statements of assurance and for identifying enterprise risks consistent with Management's Responsibility for Internal Control, COMDTINST 5200.10 (series), as well as relevant OMB and DHS Directives.

    a. Federal leaders and managers are responsible for establishing and maintaining internal controls to ensure effectiveness and efficiency of operations, reliability of reporting, and compliance with applicable laws and regulations. They are also responsible for implementing management practices that effectively identify, assess, respond, and report on risks that affect the achievement of the organization's operational and strategic goals and objectives.

    b. Risk, Risk Management, and ERM:

        (1) Risk is the effect of uncertainty on objectives; the possibility that events or circumstances might occur, which could significantly affect attainment of enterprise purpose. Risk can have either negative or positive effects; that is, not all risk is a threat, and some possible events can even result in positive outcomes.

        (2) Risk Management is a series of coordinated activities to identify and respond to potential events that may affect achievement of enterprise objectives; it seeks to identify, understand, and address significant elements of uncertainty.

        (3) ERM is an effective enterprise-wide approach to addressing the full spectrum of the organization's external and internal risks by understanding the combined impact of risks as an interrelated portfolio, rather than addressing risks only within silos. ERM provides an enterprise-wide, strategically-aligned portfolio view of organizational challenges that provides greater management awareness and insight. It involves a holistic, ongoing effort to identify, classify, and manage risks inherent to an Entity's missions, goals, and objectives. While an enterprise cannot respond to all risks related to achieving strategic objectives and performance goals, they must identify, measure, and assess risks related to mission delivery.

            (a) ERM is a real-time and agile approach to risk mitigation. When well executed, ERM can improve capacity to prioritize efforts, optimize resources, and assess changes in the

environment, helping leaders make risk-aware decisions that impact prioritization, performance and resource allocation.

(b) ERM serves to inform, and complements, the Planning, Programming, Budgeting, Execution (PPBE) process.

c. Risk Registers are standardized tools for compiling and reporting risks, they enable AOEs to document and convey their assessment and responses to identified risks. AOE risk registers also support a holistic assessment of risk across the enterprise and the compilation of Coast Guard enterprise risk portfolio, as required by Reference (a).

(1) Risk reporting should be a real-time activity. AOEs should record new risks on the Risk Register as they are identified.

(2) AOEs should involve in the Risk Register review and development process those leaders within their area of responsibility who manage significant business processes which impact the organization's operational efficiency and effectiveness.

(3) AOEs should be able to link each identified risk on their respective Risk Register to their own organizational goals or objectives.

(4) All AOEs must assess the risk associated with the misappropriation of assets in their Risk Registers, regardless of the severity. In addition to tangible assets such as capital and human resources, AOEs must also consider the risk associated with misuse of intangible assets such as proprietary information, contracts, usage rights, personally identifiable information, and other data within their systems.

(5) Changes to risks items captured on prior Risk Registers should be tracked by AOEs. Any Risk Register items that have been sufficiently mitigated and no longer need to be on the Risk Register should be archived for future reference.

d. Risk registers provide a platform that can improve communication and transparency throughout the organization, and assist in the aggregate and assessment of risk and risk-interactions across the enterprise. While Risk Registers are a required risk reporting tool utilized at the AOE level, AOEs can utilize this tool for identifying and reporting risk by all levels within their purview. Greater risk awareness and reporting allows better risk-based decisions, and is an important step in maturing the Coast Guard's ERM program.

(1) AOEs are encouraged to review, at least quarterly, their risks, relevant SOA exceptions or concerns, and assessments of current action plans for improving risk response timeliness and effectiveness.

(2) The Risk Register should be consulted to help aid and inform significant management and resourcing decision processes, such as the PPBE and Strategic Review processes.

e. Communication and transparency of risks throughout and across all levels of an organization directly contribute to the strength, maturity, and success of an ERM program. To better facilitate and further improve the Coast Guard's ERM program, an Enterprise Risk Management Working Group will be established.

f. Risk stewardship is a shared responsibility that requires the diligence of every member. It is not a separable function, but rather an essential aspect of enterprise management. It must be integral to the culture, capabilities, and practices; and applied throughout the organization.

g. Enterprise risk is managed in relation to risk appetite—the types and amount of risk, on a broad level, an entity is willing to accept in its pursuit of value. Risk appetite is within the purview of senior leadership, and serves as a guidepost for strategy formation and objective setting. It often is expressed in qualitative terms as in the Coast Guard Publication 1 discussion of the Service's Principle of Managed Risk:

We regularly honor our heritage by casting off all lines or lifting off to perform a mission that nobody else can or will attempt. We accept the fact that not every risk is within our control, and understand that a successful outcome may rest on the courage and proficiency of our people. At the same time, we also recognize that such risk must be known, respected, and minimized to the furthest extent possible.

h. Specific risks are managed with respect to risk tolerance—the level of performance variance deemed acceptable in the attainment of an established objective. Risk tolerance is generally determined at the program or unit level, where the expected variability of a particular course of action is considered with respect to both the risk appetite of the organization and the relative importance of its related objectives.

i. Risk tolerance is typically expressed either as the willingness to accept the uncertainty associated with an adopted course of action; or in the determination to treat and control the potential risk by taking steps to limit or reduce its likelihood, or constrain and mitigate its impact, or both. Risk intolerance is apparent in decisions to avoid a risk by terminating or not initiating the activity that gives rise to it; or in a decision to transfer all or part of the accompanying liability.

j. Effective risk identification ensures timely recognition and awareness of enterprise exposure to any significant new, emerging, or changing elements of uncertainty and possible impacts. This requires constant vigilance, open and frank communication, and continual engagement. Risk watchfulness and diligence must be an ingrained and habitual aspect of all organizational activity; *if you see something, say something.*

k. Internal Controls: Internal controls comprise the plans, methods, and procedures used to meet missions, goals, and objectives, and in doing so, support performance-based management. Internal controls, which are synonymous with management controls, help government program managers achieve desired results through effective stewardship of public resources. They should provide reasonable assurance that the following objectives are being achieved: effectiveness and efficiency of operations; reliability of reporting; compliance with applicable laws and regulations; and the safeguarding of assets from fraud, waste, and abuse.

(1) AOEs are responsible for taking timely and effective action to correct identified deficiencies. Correcting deficiencies is an integral part of management accountability and must be considered a priority. Corrective Action Plan (CAP) development and implementation progress should be periodically assessed and will be reported through the internal controls governance structure.

(2) Sources of information for documenting the internal control assessment include:

(a) Management knowledge gained from the daily operation of agency programs and systems;

(b) Management reviews conducted: (i) expressly for the purpose of assessing the internal control, or (ii) for other purposes with an assessment of the internal control as a by-product of the review, including annual assessments of compliance with laws and regulations and entity level controls;

(c) Office of Inspector General and GAO reports, including: audits, inspections, reviews, investigations, outcome of hotline complaints, or other products;

(d) Program evaluations, to include results of assessments, inspections, and audits (AIA);

(e) Audits of financial statements conducted pursuant to the Chief Financial Officers (CFO) Act, as amended, including: information revealed in preparing the financial statements; the auditor's reports on the financial statements, internal control, and compliance with laws and regulations; and any other materials prepared relating to the statements;

(f) Reviews of financial systems which consider whether the requirements of the Federal Financial Management Improvement Act of 1996 (FFMIA) and Appendix D of OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control, are being met;

(g) Annual evaluations and reports pursuant to the Federal Information Security Management Act (FISMA) and OMB Circular No. A-130, Managing Information as a Strategic Resource;

(h) Annual performance plans and reports pursuant to the Government Performance and Results Act (GPRA) and GPRAMA;

(i) Annual reviews and reports pursuant to the Improper Payments Elimination and Recovery Act (IPERA) of 2010 (P.L. 111-204) and Executive Order 13520, Reducing Improper Payments;

(j) Reports and other information provided by the Congressional committees of jurisdiction; and,

(k) Other reviews or reports relating to agency operations, including MISHAP reporting.

(3) The benefits of internal controls should outweigh the costs, and even the most robust internal control programs are not capable of eliminating residual risk entirely. Managers must carefully consider the appropriate balance between risk, controls, costs, and benefits in their mission-support operations. Too many controls can result in inefficiencies, while too few controls might increase risk to an unacceptable level.

l. Furthermore, a carefully constructed, utilized, and monitored ERM and internal control program will play a key role in achieving the Commandant's Guiding Principles to be Ready, Relevant, and Responsive as a service, committed to bolstering public trust in the Coast Guard. The Coast Guard "will identify enterprise risks and opportunities, and our empowered leaders will evaluate and mitigate risk where they can, and then act decisively to accomplish the mission, advance our service, and safeguard our fellow citizens" (Commandant's Guiding Principles).

12. POLICY.

a. Each AOE is responsible for providing a statement of assurance (SOA), utilizing the AOE SOA template provided in Enclosure (1). The AOE SOA must:

(1) Provide an attestation to the level of assurance over its internal controls, noting any exceptions to reasonable assurance. "Reasonable Assurance" attests that internal controls are designed to ensure efficient and effective operations, accurate reporting, compliance with laws and regulations, and prevention of misappropriation of assets within their programs. AOEs must also provide an attestation to the level of assurance that the AOE's control environment is one that promotes a commitment to integrity and ethical values, a commitment to competence, and the enforcement of accountability in accordance with the applicable GAO internal control standards, noting any applicable exceptions to this level of assurance.

(2) Validate that AOE Operational Risks have been reviewed; and optionally summarize major concerns identified from risks reported on the AOE's Operational Risk Register, which significantly affect its ability to achieve its missions, goals, or objectives.

b. Senior AOEs must assess Operational Risks reported within their control and further report a prioritized list of enterprise-level risks for consideration in the CG Enterprise Risk Register as an attachment to their SOAs. While there is no restriction to the number of enterprise-level risks to provide, a prioritized list of the top 3-5 enterprise-level risks is recommended.

c. Reporting Timeline:

(1) Senior AOEs are responsible for providing a SOA and a prioritized list of enterprise-level risks to Commandant (CG-8) no later than 29 June 2020. Additionally, they must also provide the SOAs for their Subordinate AOEs.

(2) Subordinate AOEs are responsible for providing an annual SOA to their Senior AOE no later than 15 June 2020.

(3) All other AOEs should submit their annual SOA to their parent AOE no later than 1 June 2020.

(4) While Districts, Service Centers, and Logistics Centers are not required to provide a formal SOA, AOEs who oversee them must ensure that they account for risks that might impact these units within their respective SOA.

d. Commandant (CG-8) is responsible for consolidating all reported SOAs, Risk Registers, and provided support, as well as preparing the Commandants SOA. The Commandant's SOA is due to DHS on 30 September 2020.

e. Risk Register requirements: All AOEs (Senior and Subordinate) must report their risks via the Risk Register. The Risk Register is hosted on the Commandant (CG-8) Risk Register portal, available via the Commandant (CG-85) CGPortal site: https://cg.portal.uscg.mil/units/cg85/RiskRegister/SitePages/Home.aspx. Records within the Risk Registry System would be scheduled under GENERAL RECORDS SCHEDULE 5.7: Agency Accountability Records item 010 - Internal administrative accountability and operational management control records. (DAA-GRS-2017-0008-0001)

f. Bridge Letter requirements: Although SOA submissions will occur at the end of the third quarter, it is important to gain complete coverage for the year. As such, AOEs who experience any significant changes in the degree of assurance they are able to provide over their internal controls must provide a bridge letter to Commandant (CG-8) no later than 15 September 2020 to upgrade or reduce their level of assurance. Enclosure (2) provides an example. AOEs who did not experience a significant change in their degree of assurance are not required to provide a bridge letter.

g. All AOEs listed in Paragraph 2 have member representation in the EMC-ARC, as chartered through Reference (d). The EMC-ARC will focus on AOE SOA reporting several times throughout the year:

(1) In Q3, Commandant (CG-8) will brief an overview of the SOA requirements as outlined in this annual Commandant Notice. Additionally, EMC-ARC will review and discuss the status of significant Enterprise-level risks identified in FY19.

(2) In Q3 and prior to SOA submission deadlines, Commandant (CG-8) will brief the EMC-ARC to provide additional guidance on making an assurance decision. Significant AOE risk concerns can also be discussed.

(3) In Q4, AOEs will report their findings and SOA determinations. The EMC-ARC will also formalize the CG Operational Risk Register and the recommended assurance provided in the Commandant's SOA.

h. Disclosure:

(1) Risk profiles (and by inference, Risk Registers) serve to inform the development of strategic plans as well as the President's budget, per Reference (a). They will often contain

pre-decisional, deliberative, confidential, or sensitive information and may not be releasable in response to a Freedom of Information Act (FOIA) request.

(2) However, the SOA could be made available to the public, therefore relevant information that is specifically prohibited from disclosure by any provision of law, or specifically required by Executive Order to protect the interests of national defense or the conduct of foreign affairs, must not be included in the statement made available to the public.

13. DUTIES & RESPONSIBILITIES. As defined in Management's Responsibility for Internal Control, COMDTINST 5200.10 (series).

14. FORMS/REPORTS. None.

15. REQUEST FOR CHANGES. Change requests should be submitted through the chain of command to Commandant (CG-85) at Internal-Control@uscg.mil.

CHARLES W. RAY /s/
Admiral, U. S. Coast Guard
Vice Commandant

Encl: (1) Example AOE Statement of Assurance
(2) Example AOE Bridge Letter

THIS PAGE INTENTIONALLY LEFT BLANK

EXAMPLE AOE STATEMENT OF ASSURANCE

U.S. Department of Homeland Security
United States Coast Guard

Commandant
United States Coast Guard

2703 Martin Luther King Jr. Ave SE
Washington, DC 20593-xxxx
Staff Symbol:
Phone:

5200
XX XXX 2020

MEMORANDUM

From: [AOE]

Reply to
Attn of:

To: [Senior AOE or] Commandant (CG-8)

Subj: STATEMENT OF ASSURANCE

Ref: (a) Management's Responsibility for Internal Control, COMDTINST 5200.10 (series)
(b) Coast Guard Enterprise Risk Management and Annual Statement of Assurance Reporting Requirements, COMDTNOTE 5200 of XX XXX 2020
(c) Government Accountability Office (GAO) 14-704G, Standards for Internal Control in the Federal Government (the "Green Book")

1. In accordance with references (a) and (b), I have directed an evaluation of the control activities within [AOE] in effect for the period ending (DATE). The control activities evaluated have been determined to be critical to meeting operational, compliance, reporting, and fraud prevention objectives and are in place to reduce the risk of failing to meet those objectives as outlined in enclosure (1).

2. Based on the results of this evaluation, including an assessment of applicable items listed in paragraph 10.f of reference (b), [AOE] provides **(Reasonable Assurance/Reasonable Assurance with noted exception(s)/No Assurance)** over its internal controls. Furthermore, I provide **(Reasonable Assurance/Reasonable Assurance with noted exception(s)/No Assurance)** that the control environment within [AOE] is one that promotes a commitment to integrity and ethical values, a commitment to competence, and the enforcement of accountability in accordance with reference (c).

   a. [High level summary of noted exception(s). Add additional paragraphs for each exception.]

   b. [IF APPLICABLE] A corrective action plan has been developed to address any control deficiencies in order to achieve reasonable assurance over internal controls by (DATE).

3. Additionally, my Operational Risk Register has been reviewed and updated. [OPTIONAL] I do note the following risk concerns which may significantly impact achieving [AOE] missions, goals, or objectives, which I will continue to monitor:

   a. [High level summary of noted risk concern(s). Add additional paragraphs for each area of concern.]

#

Encl: (1) Risk Management Supporting Documentation

THIS PAGE INTENTIONALLY LEFT BLANK

EXAMPLE AOE BRIDGE LETTER

U.S. Department of Homeland Security
United States Coast Guard

Commandant
United States Coast Guard

2703 Martin Luther King Jr. Ave SE
Washington, DC 20593-xxxx
Staff Symbol:
Phone:

5200
15 SEP 2020

MEMORANDUM

From: [AOE]

Reply to
Attn of:

To: Commandant (CG-8)
Thru: Commandant (CG-85)

Subj: STATEMENT OF ASSURANCE BRIDGE LETTER

Ref: (a) Management's Responsibility for Internal Control, COMDTINST 5200.10 (series)
(b) Coast Guard Enterprise Risk Management and Annual Statement of Assurance Reporting Requirements, COMDTNOTE 5200 of XX XXX 2020

1. Significant changes to our internal control program that require us to update our Statement of Assurance are outlined herein. This evaluation was conducted in accordance with references (a) and (b).

2. [Summary of changes and the revised level of assurance offered.]

#