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

Commandant
United States Coast Guard

US Coast Guard Stop 7618
2703 Martin Luther King Jr. Ave SE
Washington, DC 20593-7618
Staff Symbol: CG-85
Phone: 202-372-3445

COMDTNOTE 5200
20 MAR 2018

CANCELLED:
19 MAR 2019

COMMANDANT NOTICE 5200

Subj: COAST GUARD INTERNAL CONTROL PROGRAM ANNUAL STATEMENT OF ASSURANCE REQUIREMENTS

Ref: (a) Federal Managers' Financial Integrity Act (FMFIA) of 1982, 31 U.S.C. § 3512, (P.L. 97-255)
(b) Department of Homeland Security Financial Accountability Act (DHS FAA) of 2004, 31 U.S.C. §3516 , (P.L. 108-330)
(c) Reports Consolidation Act of 2000, 31 U.S.C. § 3516 (P.L. 106-531)
(d) Office of Management and Budget (OMB) Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control (rev. Jul 2016)
(e) Federal Financial Management Improvement Act (FFMIA) of 1996, 31 U.S.C. § 3512 (P.L. 104-208)
(f) Government Accountability Office (GAO) 14-704G, Standards for Internal Control in the Federal Government
(g) Office of Management and Budget (OMB) Circular A-11, Preparation, Submission, and Execution of the Budget (rev. Jul 2017)
(h) Chief Financial Officers Council (CFOC) and Performance Improvement Council (PIC), Playbook: Enterprise Risk Management for the U.S. Federal Government (rev. Jul 2016)
(i) Executive Management Council – Audit, Risk, and Compliance (EMC-ARC) Charter

1. PURPOSE. To identify Assessable Organizational Elements (AOE) and establish requirements that these AOEs report to the Commandant the level of assurance over the effectiveness and efficiency of control activities under their supervision and direction, to include financial and non-financial

DISTRIBUTION – SDL No.168

	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), DCO-I, DCO, DCMS

business processes. Each AOE is responsible for providing a statement of assurance (SOA) over internal controls designed to ensure efficient and effective operations, accurate reporting, compliance with laws and regulations, and prevention of misappropriation of assets within their programs. This Commandant Notice supports compliance with References (a) through (i) and directs Coast Guard managers to establish, maintain, review, and improve internal controls through active involvement in annual assessments that support the Commandant's assurance statement.

2. ACTION. The following identified AOEs have a significant impact on the Commandant's Assurance Statement and will comply with the provisions of this Commandant Notice: Director of Governmental & Public Affairs (CG-092); Judge Advocate General & Chief Counsel (CG-094); Assistant Commandant for Human Resources (CG-1); Director of Health, Safety & Work-Life (CG-11); Director of Civilian Human Resources, Diversity & Leadership (CG-12), Director of Reserve & Military Personnel (CG-13); 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 Resources/Chief Financial Officer (CG-8); Assistant Commandant for Acquisition/Chief Acquisition Officer (CG-9); Senior Procurement Executive & Head of Contracting Activity (CG-91); Deputy Commandant for Operations (DCO); Deputy Commandant for Mission Support (DCMS); Director of International Affairs & Foreign Policy (DCO-I); Director of Operational Logistics (DOL); Commander, Force Readiness Command (FORCECOM); Commander, Coast Guard Atlantic Area (LANT-00); and Commander, Coast Guard Pacific Area (PAC-00). Internet release is authorized.

3. DIRECTIVES AFFECTED. COMDTNOTE 5200 dated 28 Mar 2017 is hereby cancelled.

4. BACKGROUND.

   a. Risk is the effect of uncertainty on objectives. Risk management directs and controls challenges or threats to achieving organizational goals and objectives. Risks arise from a variety of external and internal environments. Examples include economic, operational, and organizational change factors, all of which would negatively impact an Agency's ability to meet goals and objectives if not resolved.

   b. Enterprise Risk Management (ERM) involves a holistic, ongoing effort to identify, classify, and manage risks inherent to an Entity's missions, goals, and objectives. ERM is a tool that allows an organization to identify controllable risks and take the appropriate action to improve performance over future periods, and to identify and address the full spectrum of an organization's significant external and internal risks or opportunities that merit additional organizational measures to maximize performance. ERM improves on classical methods of management, offering a better approach to determining where to focus risk mitigation efforts and where risk can be accepted in order to gain efficiencies.

   c. Reference (d) requires agencies to implement ERM programs, a key component of which is the management of risk through 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. Furthermore, a carefully constructed, utilized, and monitored internal control program will play a key role in achieving the Commandant's Commitment to Excellence Priority #2: to "ensure efficiency across all Coast Guard activities through effective planning and sound risk management."

d. ERM compliments the Planning, Programming, Budgeting, Execution (PPBE) process. While the PPBE process already plays a large role in identifying significant organizational risks, it is done through the longer lens of a 2-year outlook. ERM is a real-time and agile approach to risk mitigation. When well executed, ERM improves 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.

e. The Commandant's Assurance Statement is submitted annually and must include specific assurances regarding the Coast Guard's internal control program. While assurances provided by AOEs may only concentrate on a segment of these 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) Pursuant to Reference (a) Section 2, (commonly referred to as Section 2 of the Integrity Act), the Assurance Statement must include a statement asserting or denying a reasonable assurance that the Coast Guard's controls are achieving their intended objectives, and a report on any existing material weaknesses in the controls. Exceptions to assurance that would be determined to be significant enough to report outside of the organization 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) Reference (b), Section 4 (c), requires assurance of internal controls that apply to financial reporting by DHS. The Coast Guard will evaluate the corrective actions being taken to resolve any inadequacies in its internal controls over financial reporting (ICOFR) program within the current year and will assess whether previously reported material weaknesses continue to exist. The Coast Guard's focus will be on adequately executing corrective

actions in areas where controls are ineffective in achieving their goal of curtailing unaccepted risk. In addition, management is required to identify significant financial reporting areas where assurance can be provided by conducting tests of operating effectiveness of internal controls. The Commandant's ICOFR assessment is based on the results of the Coast Guard's control testing and assessments. It includes a description of each reportable condition as well as a determination as to whether the reportable condition rises to the level of a material weakness. Testing results reported by the Office of Internal Controls, Commandant (CG-85) are a large factor in the reported assurance in this Section.

(3) Pursuant to Reference (a), Section 4, the Commandant's assurance statement includes an assessment of Coast Guard financial management systems' conformity with government-wide requirements. If these systems do not substantially conform to financial system requirements, the statement must list the nonconformities and discuss plans for bringing its systems 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) Pursuant to Reference (c), and to support the Secretary's assurance statement over performance information, the Coast Guard must provide reasonable assurance that the mission performance data reported to DHS is complete and reliable. In instances where such assurance can't be provided, the Coast Guard must identify any material inadequacy in the data. The DHS Government Performance and Results Act (GPRA) Performance Measures Checklist for Completeness and Reliability is used to self-evaluate key controls over GPRA performance measure planning and reporting information. The results of any DHS independent verification and validation assessments, as well as any Coast Guard-led internal measure reviews, should be factored into the ratings on the checklist.

f. While this Commandant Notice outlines an annual reporting requirement, Reference (g) identifies a best practice to conduct frequent data-driven reviews to better manage risks to better achieve operational, compliance, and reporting objectives. Reference (h) expands 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. To help facilitate this, quarterly reviews of risks, relevant SOA exceptions or concerns, and assessments of current action plans are encouraged for improving risk response timeliness and effectiveness.

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. 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 Instruction 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 policies in this Instruction 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.

7. 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://cgportal2.uscg.mil/library/directives/SitePages/Home.aspx.

8. PROCEDURE. Specific procedures for complying with this Commandant Notice can be found in the Statement of Assurance Process Guide on the Commandant (CG-85) CGPortal Page: https://cgportal2.uscg.mil/units/cg85/SitePages/Home.aspx.

9. 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.

10. DISCUSSION. This Commandant Notice lays out the specific deliverables for completing the SOA and Risk Register requirements set forth in Management's Responsibility for Internal Control, COMDTINST 5200.10 (series).

a. The primary objective of the SOA and Risk Register process is to identify risks to organizational goals and objectives relating to its operations, compliance, and reporting. A secondary objective of this process is, from the risks identified in the primary objective, to identify risks to the organizational strategic objectives. The Risk Register is the standardized organizational reporting and monitoring tool through which the internal control governance structure can communicate and raise visibility of the risks within each and across organizational silos.

b. Assessing risk and control effectiveness: To ensure balance between controls and risk in programs and operations, managers must first assess risk and the adequacy of the controls currently in place to reduce those risks.

(1) Inherent risk is the risk to the achievement of entity objectives in the absence of any actions management might take to reduce the risk's likelihood and/or impact. For the purposes of the Coast Guard internal control program, inherent risk is measured on a 1-10 scale and represents the worst case scenario if a particular risk was left completely uncontrolled.

Because it measures risk in a hypothetical environment, inherent risk can be difficult to assess and requires careful analysis and collaboration among stakeholders.

(2) Residual risk represents the risk that exists in the current environment with existing controls in place, operating at their actual level of effectiveness and not necessarily their designed level of effectiveness. The Coast Guard internal control program measures residual risk as a function of the risk's likelihood and impact.

(a) "Likelihood" represents the probability that a given event will occur and is measured as a percentage chance of occurrence.

(b) "Impact" represents the severity or seriousness of a negative effect resulting from the occurrence of a given event.

(3) Control effectiveness is the amount of risk mitigated by a particular control.

(4) Risk tolerance is the acceptable level of variation in performance relative to the achievement of objectives. While the Coast Guard has not defined the organization's risk tolerance as an Enterprise, AOEs should work to define risk tolerance within their specific span of control.

c. Assessing inherent risk in addition to residual risk can assist the organization in understanding the effectiveness of their current controls as well as the extent of additional risk responses needed.

d. Sources of Information: Reference (d) recommends that agencies integrate and coordinate internal control assessments with other internal control-related activities. Further, OMB provides that the assessment of internal controls can be performed using a variety of information sources. AOEs should consider the following when determining the level of assurance to provide in their SOA, as applicable:

(1) Management knowledge gained from the daily operation of agency programs and systems as analyzed and documented through an annual risk assessment process;

(2) Management reviews conducted expressly for the purpose of assessing the internal control, or 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;

(3) Inspector General and Government Accountability Office reports, to include audits, inspections, reviews, investigations, outcome of hotline complaints, or other products;

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

(5) Audits of financial statements conducted pursuant to the Chief Financial Officers (CFO) Act of 1990, 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;

(6) Reviews of financial systems which consider whether the requirements of Reference (e) and Appendix D of Reference (d) are being met;

(7) Annual evaluations and reports pursuant to the Federal Information Security Management Act (FISMA) and OMB Circular No. A-130, Management of Federal Information Resources;

(8) Annual performance plans and reports pursuant to GPRA;

(9) Annual reviews and reports pursuant to the Improper Payments Information Act (IPIA) as amended by the Improper Payments Elimination and Recovery Act and Executive Order 13520, Reducing Improper Payments;

(10) Single Audit Act reports for grant-making agencies;

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

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

e. 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 should consider the quantitative and qualitative aspects of their tolerance for risk in determining where to devote finite resources toward risk reduction and should make note of risks they choose to accept.

f. The risk assessment also serves as a tool for AOEs to identify opportunities to operate more efficiently, particularly in a limited budget environment. The identification of low impact and/or low likelihood risks shouldn't be overlooked, as scarce resources expended on managing these risks might be available for reallocation toward more significant risks. Doing so will continue to ensure that the Coast Guard is managing risks effectively and efficiently across the entity's risk profile.

11. POLICY.

a. Deputy Commandants, Area Commanders, and Vice Commandant's AOE direct-reports (specifically CG-8, CG-092, and CG-094) are responsible for providing an SOA for internal controls and compliance with laws and regulations to Commandant (CG-8) no later than 27 July 2018.

b. In addition to the sources of information listed in Paragraph 10.d, AOEs should consider the risks identified and assurances provided by AOEs subordinate to them when determining the level of assurance to provide in their SOA. This is an important part of the assurance process since numerous minor risks across a portion of the organization could result in a much higher level of risk in aggregate. The senior-level SOAs identified in Paragraph 11.a must include the SOAs of all AOEs subordinate to them as enclosures. In order to facilitate this:

(1) AOEs that report directly to an AOE listed in Paragraph 11.a are responsible for providing an annual SOA for internal controls and compliance with laws and regulations to their senior AOE no later than 13 July 2018.

(2) All other AOEs should submit their annual SOA to their senior AOE no later than 29 June 2018.

(3) While Service 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 Statements of Assurance.

c. The SOA memo explicitly states the level of assurance that can be made with regard to the effectiveness of control activities under an AOE's supervision and direction. In addition, AOEs will provide assurance regarding the commitment to integrity, competence, and the enforcement of accountability within their programs, which are critical to maintaining an effective control environment per Reference (f).

d. At a minimum, AOEs should identify exceptions within their SOA when they merit the attention of the Commandant and/or meet any of the criteria outlined in Paragraph 4.e.(1).

e. The assurance statement must be supported and documented with a high-level risk assessment utilizing the Commandant (CG-8) Risk Register template, which is available on the Commandant (CG-85) CG Portal site: http://cglink.uscg.mil/f69c70f9

f. The Risk Register enables AOEs to document their process for identifying, assessing, and responding to risk as required by Reference (d). 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.

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

(2) A significant risk is one in which the negative impact as outlined in Paragraph 4.e.(1) is at least a reasonable possibility. Not all risks documented on the Risk Register will be significant, but a significant risk would impact the level of assurance provided. Risks that impact defined Coast Guard strategic objectives should have an impact assessment rating that reflects the elevated focus.

(3) 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 data systems.

(4) Risks identified within the Risk Register should be assessed (quantified) at the directorate level when applicable. For example, Commandant (CG-11) would make risk rating

determinations (to include whether it is internal or external in nature) from the perspective of Commandant (CG-1).

(5) The Risk Register utilizes a categorization system to group the risks for macro-level analysis. AOEs that identify risks which do not fit into existing categories may submit requests for additions, deletions, and improvements via their representative to the Internal Control Working Group (ICWG), which functions as the action officer component of the Coast Guard's Internal Control governance structure.

(6) Changes to risks items captured on prior Risk Registers should be tracked by AOEs on the current Risk Register template. Any Risk Register items that have been sufficiently mitigated and no longer need to be on the Risk Register should be recorded on the "Removed Risk Items" tab of the Risk Register Template.

(7) AOEs will also be required to identify the specific planned response; to include reducing, sharing, avoiding, or accepting the risk.

(8) Deputy Commandants, Area Commanders, and Vice Commandant's AOE direct-reports (specifically CG-8, CG-092, and CG-094) should target approximately 5-10 risks within their Risk Registers that they believe would have the greatest impact on the Commandant's Statement of Assurance, considering the aggregated top risks reported by their subordinate AOEs. This provision is not intended to be arbitrarily restrictive in nature, but serves as a guideline to facilitate the collaborative process between Commandant (CG-8) and other AOEs in composing a single, succinct Risk Register for submission to the Commandant.

g. Enclosure (1) provides an example SOA that includes the minimum language required. AOEs may tailor additional language if needed to articulate exceptions or corrective actions. Each SOA will feed the Commandant's assurance statement which is due to the DHS on 28 September 2018.

h. 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 14 September 2018 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.

i. The Executive Management Council – Audit, Risk, and Compliance (EMC-ARC) Board, as chartered through Reference (i), will focus on AOE SOA reporting four times throughout the year.

(1) In Q1/Q2, Commandant (CG-8) will brief an overview of the SOA requirements as outlined in this annual Commandant Notice.

(2) In Q3 and prior to SOA submission deadlines, Commandant (CG-85) 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 recommended assurance provided in the Commandant's Statement of Assurance.

j. 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 throughout the internal controls governance structure.

k. Disclosure:

(1) Per Reference (d), risk profiles (and by inference, risk registers) serve to inform the development of strategic plans as well as the President's budget. They will often contain pre-decisional, deliberative, confidential, or sensitive information and may not be releasable in response to a FOIA request.

(2) However, the Statement of Assurance 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.

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

13. FORMS/REPORTS. None.

14. REQUEST FOR CHANGES. Change requests should be submitted through the chain of command to Commandant (CG-85).

C. D. MICHEL /s/
Admiral, U. S. Coast Guard
Vice Commandant

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

EXAMPLE AOE STATEMENT OF ASSURANCE

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

Commandant
United States Coast Guard

US Coast Guard Stop 7618
2703 Martin Luther King Jr. Ave SE
Washington, DC 20593-7618
Staff Symbol:
Phone:

5200
XX XXX 2018

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 Internal Control Program Annual Statement of Assurance Requirements, COMDTNOTE 5200 of XX XXX 2018
(c) Government Accountability Office (GAO) 14-704G, Standards for Internal Control in the Federal Government

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.c. 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].

3. [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).

#

Encl: (1) Risk Management Supporting Documentation

Copy: Commandant (CG-85)

EXAMPLE AOE BRIDGE LETTER

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

Commandant
United States Coast Guard

US Coast Guard Stop 7618
2703 Martin Luther King Jr. Ave SE
Washington, DC 20593-7618
Staff Symbol:
Phone:

5200
14 SEP 2018

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 Internal Control Program Annual Statement of Assurance Requirements, COMDTNOTE 5200 of XX XXX 2018

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.]

#