



Commandant
United States Coast Guard

2100 Second Street, S.W.
Washington, DC 20593-0001
Staff Symbol: CG-861
Phone: (202) 372-3700
Fax: (202) 372-3950

COMDTINST 5512.2
NOV 09, 2006

COMMANDANT INSTRUCTION 5512.2

Subj: COAST GUARD CREDENTIALS AND BADGES

1. **PURPOSE.** This Instruction outlines United States Coast Guard (USCG) policy for the procurement, issue, control, and disposition of USCG Credentials and Badges.
2. **ACTION.** Area and district commanders, commanders of maintenance and logistics commands, commanding officers of headquarters units, assistant commandants for directorates, Judge Advocate General, and special staff offices at Headquarters shall ensure compliance with the provisions of this Instruction. Internet release authorized.
3. **DIRECTIVES AFFECTED.** Intelligence Officer Credentials and Badges, COMDTINST 5512.11, and Marine Investigator Badges and Credentials, COMDTINST 16700.8 are cancelled and superseded by this Instruction. The Physical Security and Force Protection Program, COMDTINST M5530.1C (Chapter 10), is limited by the provisions of this Instruction. All policies regarding credentials outlined in this Instruction supersede any relevant provisions in that Manual.
4. **BACKGROUND.** Certain Coast Guard operations are facilitated by the use of special identification documents hereafter referred to as Credentials. These Credentials are issued to selected and appropriately qualified USCG members. They are used to interact with the public; conduct inquiries, investigations and other legal activities; conduct inspections; and to coordinate or conduct liaison with federal, state, and local agencies. Currently, the Coast Guard employs several different types of Credentials to support a variety of operational and investigative purposes. On 31 March 2004, the Department of Homeland Security (DHS) issued specific guidance that mandates standardization of credentials used by DHS organizational elements. This Instruction, therefore, is designed to bring the USCG into full compliance with, and to amplify, that new guidance.

DISTRIBUTION – SDL No. 146

	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	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
B	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
C	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
D	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
E	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
F																	1	1	1							
G		1	1	1	1																					
H																										

NON-STANDARD DISTRIBUTION:

5. AUTHORITY. This Instruction complies with guidelines found in the following references:
 - a. Homeland Security Act 2002, codified in 6 USC
 - b. 5 USC §556(c) and 33 CFR 20.202
 - c. 6 USC §113, 122
 - d. 14 USC §89, §95, §98, §143
 - e. 19 USC §1409
 - f. 46 USC §63, §77
 - g. EO 12333
 - h. EO 12958
 - i. DON EKMS 1 and 3A
6. IMPACT. Coast Guard programs that currently issue and control Credentials may have to make adjustments to comply with these provisions, but their ability to issue appropriate credentials is unaffected. Those programs that anticipate a need to issue Credentials will benefit from this policy guidance regarding how to seek approval and how to administer such a program.
7. DEFINITIONS.
 - a. Badge: A serial numbered metal or metal-like emblem that connotes an official level of law enforcement, or investigative authority, to the bearer or wearer.
 - b. Credential: Any document that is presented to a requestor to verify the holder's status and authority to perform a specialized role, and which enjoins those to whom it is presented to fully cooperate with the bearer.
 - c. Credentials Custodian: The person designated by a Program Manager to maintain possession of, issue and control USCG Credentials.
 - d. Badge and Credential (B&C): The document and an accompanying badge which serve as both a form of identification (Credential) to verify the holder's status to perform a specialized role, and which also empowers the bearer with a level of law enforcement or investigative authority (Badge).
 - e. Representative Credentials: The document (without a badge) which identifies the bearer as a duly appointed and accredited representative of the Department of Homeland Security and USCG to perform a specialized role, and which enjoins those to whom it is presented to fully cooperate in that role.

- f. Administrative Law Judge Credential: The singular type of Authority Credential issued to Administrative Law Judges which both identify's that person as a USCG Administrative Law Judge (ALJ) and which indicates his/her authority pursuant to that appointment.
 - g. Program Manager: The designated Office Chief or Director with responsibility to ensure that this policy is applied and adhered to by all personnel engaged in an activity supporting that program's mission area of responsibility.
8. APPROVED CREDENTIALS. USCG has identified the need for four types of Credentials: Police Badges (without credentials), Badges and Credentials (B&C), Representative Credentials and ALJ Credentials.
- a. Police Badges: These are issued only to USCG members who serve as police officers at one of six Coast Guard installations that have such forces (i.e., USCG Academy, TRACEN Cape May, TRACEN Petaluma, ISC Kodiak, USCG Sector New York, and USCG Yard Baltimore). These USCG forces must have undergone specialized police training at an accredited police-training center or, as a minimum, completed the Personnel Qualification Standard (PQS) for police officer duties.
 - b. Badges and Credentials (B&C): These Credentials are issued only to:
 - (1) Special Agents of the Coast Guard Investigative Service (CGIS) who perform criminal investigations, personal protection duties, and Law Enforcement (LE) intelligence duties.
 - (2) Intelligence Officers who perform liaison, oversight and support to intelligence investigations.
 - (3) Coast Guard Counterintelligence Service (CGCIS) Counterintelligence Agents who perform counterintelligence (CI) functions.
 - (4) Qualified Marine Investigators who conduct investigations into marine casualties, violations of law/regulation by Coast Guard credentialed mariners, and other regulatory marine investigations.
 - (5) Certified Electronic Keying Material (EKMS) Inspectors who perform inspections of the USCG EKMS program under U.S. Navy auspices.
 - (6) Drivers/Aides that transport and otherwise support the Commandant and other USCG senior leadership.
 - c. Representative Credentials: These Credentials (document only) are issued to:
 - (1) USCG members who perform intelligence functions such as collection and liaison with other national intelligence agencies.
 - (2) USCG Security Managers who conduct security evaluations at installations.

- (3) Security personnel who perform technical security functions, such as Technical Surveillance Countermeasures (TSCM).
- (4) Administrative law personnel who support Administrative Law Judges to facilitate access to the court system.
- (5) USCG officers and contractor personnel who perform Intelligence or Counterintelligence functions.

d. ALJ Authority Credentials: These Credentials are issued to Coast Guard Administrative Law Judges who preside over administrative hearings for the Coast Guard and other DHS agencies.

9. **RESPONSIBILITIES.** The USCG Credentials and Badges Program is characterized by centralized oversight, audit, and policy with decentralized management (i.e., production and issue) for the various program elements. Overall policy development, program management, and audit authority of the Coast Guard Credentials and Badges Program has been vested in the Assistant Commandant for Planning, Resources, and Procurement, (CG-8). The Office of Security Policy and Management, (CG-86), is the action office within Commandant (CG-8) for this program. Responsibilities for the management of the various program elements that comprise the USCG Credentials and Badges Program are designated as follows:

a. Assistant Commandant for Intelligence and Investigations (CG-2):

- (1) Oversees the Badges and Credentials produced, issued and accounted for by the Director, Coast Guard Investigative Service (CG-2-CGIS). CGIS Badges and Credentials (B&C) are issued to CGIS Special Agents. Badges and Credentials are also issued to Drivers/Aides that support the Commandant and senior leadership.
- (2) Oversees the Badges and Credentials produced, issued, and accounted for by the Chief, Office of Intelligence Security Management (CG-22). These Badges and Credentials or Representative Credentials (as appropriate) are issued to Coast Guard Intelligence Officers.
- (3) Oversees the Badges and Credentials produced, issued, and accounted for by the Coast Guard Counterintelligence Service (CGCIS). These Badges and Credentials or Representative Credentials (as appropriate) are issued to: CGCIS Counterintelligence Agents, CI Officers, and selected supporting contractors.

b. Assistant Commandant for Command, Control, Communications, Computers and Information Technology (CG-6): Oversees the Badge and Credentials produced, issued, and accounted for by the Chief, Office of Communications Systems, (CG-62). These Badge and Credentials are issued to USCG Certified Electronic Keying Material System (EKMS) Inspectors who operate under agreement with, and supervision of the Department of the Navy EKMS Program.

c. Assistant Commandant for Planning, Resources, and Procurement (CG-8):

- (1) Serves as the overall program manager for policy and procedures and oversight relating to the USCG Credential Program.
 - (2) Oversees the Credentials produced, issued and accounted for by the Chief, Office of Security Policy and Management, (CG-86). These Badges or Representative Credentials (as appropriate) are issued to Coast Guard Police Forces, Security Managers, and TSCM Technicians.
- d. Assistant Commandant for Prevention (CG-3P): Oversees the Credentials produced, issued and accounted for by the Chief, Office of Investigations and Analysis (CG-3PCA). These Badges and Credentials are issued to Coast Guard Marine Investigators.
 - e. Chief Administrative Law Judge, (CG-00J): Produces, issues, and accounts for the ALJ Authority Credentials and Representative Credentials issued to Administrative Law Judges and legal staff respectively.
 - f. Unit Commanders: Are responsible for controlling and safeguarding Credentials assigned to their organizations. In this capacity, they must ensure that Program Managers have the resources to properly secure or safeguard and account for Credentials within their Area of Responsibility.
 - g. Program Managers:
 - (1) Issue individual Program Implementation Guidance for this Instruction.
 - (2) Obtain a legal review from the Judge Advocate General of the Coast Guard, (CG-094), to ensure legal sufficiency of the authority that will be the focus of the Credential. Credentials are representational in nature. Issuance must be supported by underlying legal authorities, and must occur only to individuals meeting specified criteria, as appropriate given the program, and consistent with the underlying legal basis.
 - h. Credentials Custodians: Program Managers of each program authorized to issue USCG Credentials Program will appoint a Credentials Custodian. This individual is responsible for the production, receipt, issue, replacement and routine accountability for Credentials in that program element. The names and contact data for Credentials Custodians will be forwarded to Commandant (CG-86).
 - i. Individual Bearer: The individual to whom a Credential is entrusted is at all times responsible for safeguarding them, unless relieved of such responsibility by the Credentials Custodian.
10. USE. Credentials are for the sole purpose of identifying the bearer as a duly appointed/accredited representative of the U.S. Coast Guard who is performing a specific duty, and within the limits of a specific authority. Further, as defined in paragraph 5, badges alone and those credentials, which contain a badge in addition to a paper credential, are herein distinguished from Representative Credentials with regard to the level of authority conveyed respectively in them. USCG has determined that by both statute and practice within the law enforcement community, and social custom in society, badges are generally recognized to have some degree of statutorily supported law

enforcement/investigative authority, (i.e., the authority to issue citations/fines, investigate crimes and maritime casualties, and apprehend or detain an individual). Therefore, only persons who have undergone formal law enforcement, investigative training/certification, and whose duties require the conduct of police, investigatory functions that are supported by law will be issued badges.

11. CERTIFICATION. Program Managers will ensure that Credentials are only issued to Coast Guard Personnel (uniformed or civilian) or supporting contractors who have demonstrated requisite competence in the functional area for which they are required, and the maturity to judiciously exercise the authority specified in the credential. Requisite competence is herein defined as meeting specific written standards for the duties performed. Program Managers will maintain a certification that the individual issued a credential has completed the requisite training (formal schools or on the job training (OJT)) and met the program standards to qualify them for performing the specified duties. That certification will also include a validation that the bearer has been briefed on the limits of the authority specified in the credential and the actions or behaviors that constitute possible abuse of that authority IAW Paragraph 16.
12. ISSUANCE AND PRODUCTION PROCESS. Program managers will prepare credential application packets as follows:
 - a. Individual credentials will be prepared utilizing DHS-approved serial numbered credential card stock, and in accordance with DHS design guidelines.
 - b. Credentials proofs will contain the individual bearers name, color photograph, and job title (see Enclosure (1) for example). They will also be signed by the bearer.
 - c. Program Managers will ensure security lamination of the approved credential using the approved DHS lamination sleeve. Credentials will be placed in a leather holder, and a serial-numbered badge affixed, if required.
 - d. Program Credentials Custodians will issue completed credentials using a receipt system and log the issue data in their accountability database.
13. REISSUE/REPLACEMENT. Credentials may require replacement for a number of reasons including: fair wear and tear, mutilation, loss or theft, name change, and/or a significant change in physical appearance of the bearer. A brief discussion of each circumstance wherein replacement of an Credential may be required as follows:
 - a. Unserviceable Credentials: Although designed to remain serviceable for a long period of time, USCG Credentials may require replacement due to normal wear and tear, or damage. In such cases, where a Program Manager determines that a Credential has become unserviceable, that manager should direct the Credentials Custodian to issue a replacement to the bearer. Normally, if the Credential also includes a Badge, that component will likely remain serviceable and can therefore be incorporated into the new Credential. When this occurs, the Program Manager, through the custodian, will ensure the destruction of the unserviceable Credential in the same manner as a classified document. The responsible custodian will also annotate the inventory records or databases, as appropriate, to reflect both the destruction of the old Credential and the

issue of the new one. A copy of that updated inventory and a certificate of destruction will be maintained by the custodian with the inventory records or databases.

- b. Loss/Theft: Upon discovery that a Credential has been lost or stolen, the bearer of that Credential will immediately notify his/her direct supervisor. The individual's organization will take the following immediate actions:
 - (1) Conduct a comprehensive search to recover the lost or stolen Credential.
 - (2) Notify the responsible Program Credentials Custodian of the loss, who will, in turn notify the Program Manager. The Program Manager will notify Commandant (CG-86), within 48 hours. Commandant (CG-86) will notify the DHS Office of Security by official message in accordance with (IAW) DHS MD 11010.1, "Issuance and Control of Credentials." The message will include approximate time and date the credential was discovered missing and the location where the credential was last seen.
 - (3) Conduct an inquiry into the circumstances of the loss. Loss due to negligence or carelessness may be grounds for disciplinary action.
 - (4) Notify CGIS. CGIS notification will be in writing via message to Commandant (CG-2-CGIS). CGIS will notify the National Crime Information Center (NCIC), within 24 hours of the supervisor's notification. Reports of loss should contain a detailed description of the Credential, date of loss, and the location where lost. In those cases where lost, missing or stolen credentials are recovered, commands must also notify Commandant (CG-2-CGIS) via message of the recovery in order to ensure, per NCIC and DOJ regulations, that the report of missing item is removed from NCIC.
 - (5) Provide to Commandant (CG-86) within 30 days of the incident a summary of the inquiry regarding the loss or theft and any actions taken relating to the bearer. If the Credential is not recovered, submit a request for relief of accountability to the Program Manager with copy to Commandant (CG-86). Such relief should only be granted by Program Managers when it has been determined that the lost Credential cannot, or likely will not, be recovered.
- c. Name Change: Credentials will be replaced when the bearer undergoes a name change either as result of marriage or due to a legal name change action.
- d. Change in Appearance: When a dramatic change in physical appearance of the bearer occurs, a new Credential will be issued. This category includes but is not limited to a significant change in weight, change of hair color, addition or deletion of facial hair, etc.

14. RETENTION/EXPIRATION. Credentials are issued only to support a specific duty. When the bearer of a Credential has been reassigned to other duties, relieved for cause, retired, or deceased, the Credential is expired for that person and will be turned in to the appropriate Credentials Custodian. Program Managers will ensure that commanders require bearers to turn in their Credentials as part of their mandatory unit out-processing procedures. Expired credentials will be stamped "EXPIRED" or "RETIRED" with permanent ink or perforations before being returned to prior bearers as a memento

for retirement, separation, or special recognition. Mementos will be documented on the Letter of Certification and kept on file IAW paragraph 15. (It is also recommended that Credentials be turned in to the custodian for temporary safekeeping when the bearer is hospitalized for a protracted period, or when traveling outside the United States not on official business.)

15. RECORDS. The Program Managers will maintain all Program Manager Letters of Certification, and records of retirement and destruction of Credentials IAW Schedule 18 of the General Records Schedule.

16. MISUSE.

a. Use of USCG Credentials for other than their intended purpose or when other means of identification (i.e., a USCG Identification Card) would be more appropriate is considered an abuse and may be grounds for revocation of the Credential, removal of the bearer from the duties that require Credentials, and other disciplinary action. USCG members who have knowledge of an alleged abuse are responsible for reporting it to their chain of command. The following are additional examples of what may constitute abuse of Credentials:

- (1) Alteration or tampering with Credentials.
- (2) Photocopying, or copying of Credentials.
- (3) Using a Credential to present oneself as a Law Enforcement Official beyond the scope of the authority specified for that Credential.
- (4) Using a Credential to gain access to areas/facilities or information not warranted by the authority specified in the Credential.
- (5) Using a Credential to garner some privilege or special access while off-duty.
- (6) Using a Credential in an attempt to avoid a legal citation (i.e., parking ticket).

b. When a possible abuse of Credentials has been reported, the Program Manager responsible for the element that has custodial responsibility for that Credential will:

- (1) Initiate an administrative inquiry concerning the allegation of abuse, and report the incident to Commandant (CG-86).
- (2) Consider withdrawing the Credential of the alleged abuser, pending completion of the investigation.
- (3) Refer the case to CGIS, if criminal intent or activity is indicated.
- (4) Consider a request to the commander with non-judicial authority over the alleged abuser to take non-judicial action or refer the matter for judicial action, if the investigation substantiates the allegation of abuse.

- (5) Provide a detailed report to Commandant (CG-86) concerning the findings and outcome of the investigation within 30 days of completion.

Note: Credentials are not designed to replace the normal USCG Identification Card, Common Access Card (CAC) or security badges issued at installations. Credentials are a supplement to those forms of identification; therefore, under most circumstances, the bearers of Credentials are expected to carry their normal CG identity papers as well, as required by local policy. Credentials are also not designed to supplant those one-time Letters of Appointment that may be used by investigating officers conducting a single (Commander's) inquiry.

17. MINIMUM CONTROLS AND SAFEGUARDING. Credentials are the property of the United States Coast Guard. Although they are not classified, Credentials contain extremely sensitive information that will cause a security concern if they fall into the wrong hands. In view of this, they should be safeguarded when carried on the person (i.e., fastened with a clip or properly secured in a pocket, purse, etc.) and when in storage, Credentials Custodians will accord them the same degree of security as a For Official Use Only (FOUO) document. They will be secured IAW procedures in the Classified Information Program Management, COMDTINST M5510.23 (series), for FOUO information. Minimum controls for Credential accountability are as follows:

- a. **Design:** Credentials and Badges must be unique. Each Credential will be serial numbered. Minimum design requirements are the following: Name, DHS Department (i.e., U.S. Coast Guard), and duty appointment or position title. Department of Homeland Security minimum design requirements include a DHS seal and the DHS Secretary's signature line, as shown in Enclosure (1).
- b. **Accountability:** Program Managers are responsible for accountability of credentials issued for their program. In order to fulfill their accountability responsibilities Program Managers will:
 - (1) Maintain an electronic database for their program element with identifying data corresponding to each credential issued. That list will include as a minimum: Name, Duty Assignment, Certification Date, Date of Issue, Approving Authority for Issuance, Serial Number(s) (Credential and when appropriate accompanying Badge) and a copy of the individual bearer's photograph which appears on the Credential (when that capability becomes available). In accordance with information technology best practice a back-up file will also be maintained.
 - (2) A copy of each program element master credentials list will be provided to Commandant (CG-86) on completion of the program annual inventory.
 - (3) In those instances where the identity of the bearer of a credential is sensitive (law enforcement, intelligence or counterintelligence), Program Managers will take appropriate action to limit access to their database consistent with identified security requirements. Copies of program master lists forwarded to Commandant (CG-86) that contain the names of such protected individuals will be edited to satisfy security requirements. Program Managers

will, however, certify to Commandant (CG-86) the number of credentials issued to persons in a protected status.

- c. Control: Whenever a new Credential is issued, an old, unserviceable or lost one is replaced, or any change in physical possession of the credential occurs, a written receipt system will be used by the Credential Custodian to maintain accountability and transfer responsibility for custody.
- d. Transmission: Apart from direct personal transfer, Credentials may be forwarded using approved government courier services that permit electronic tracking or registered U.S. Mail.
- e. Inventory: Upon change of Program Element Manager or Credentials Custodian, a 100% inventory of all credentials assigned to that program element will be conducted. Such inventories will also be conducted annually. Reports of annual inventories will be made to Commandant (CG-86) no later than the fifth working day of the fiscal year. Additional inventories may also be required when requested by the DHS Office of the Inspector General (IG), as part of the IG Internal Controls or Audit Program.
- f. Audit: Commandant (CG-86) will fulfill its program management oversight responsibilities by conducting annual audits of each credential program element. Audits will be short notice. An outline of the scope of these audits is contained in Enclosure (2). A sample checklist for the annual audit is contained in Enclosure (3). In accordance with auditing best practices, the Commandant (CG-86) auditor(s) will examine compliance with the provisions of this instruction, overall accountability, and internal controls.

18. REQUEST TO ESTABLISH A NEW CREDENTIAL PROGRAM.

- a. Justification: Requests for new Credential Programs will be made in writing to Commandant (CG-86). Program Managers who have identified a requirement for a new Credential must substantiate the need for that Credential based on operational effectiveness criteria. Justification will also include reference to the statute, executive order, presidential, DHS Management Directive, USCG Instruction, or other legal basis cited as authority to perform the duties specified in the proposed credential.
- b. Request: The request will include a graphic representation of the proposed credential (to include associated badge or a statement that no badge will accompany the document) as well as a detailed description of the implementing procedures that the program manager will use to ensure the integrity of the system.
- c. Legal Review: Program Managers will also obtain a legal review from The Judge Advocate General of the Coast Guard (CG-094) to ensure legal sufficiency of the authority that will be the focus of the Credential. Credentials are representational in nature and must be substantiated by underlying law.
- d. Approval Process: Requests for new Credentials with accompanying justification will be forwarded to Commandant (CG-86) for coordination staffing. Commandant (CG-86) will review the request package for completeness and facilitate executive level review via the Intelligence,

Security, Law Enforcement Policy (ISLP) Council. The ISLP Council will validate the effort of the program manager and provide an opinion to the Chief of Staff regarding the request. The Commandant, through the Chief of Staff, is the approving authority for Credential Programs.

19. REPORTS.

- a. Initial: Each approved program element will provide Commandant (CG-86) with an accounting of what Credentials and Badges have been issued, to whom, Coast Guard wide within 30 days of the effectiveness of this instruction.
- b. Annually: The initial accounting will be updated, and reported on an annual basis as indicated in paragraph 17 E. Discrepancies in inventory findings will be fully explained.
- c. As Required: Reports of lost, stolen, damaged or replaced Credentials will be made in accordance with paragraph 13.

20. DATA ACCESS AND VALIDATION. As previously noted, Credentials are a form of official identification. While the intent of their use is to establish the bona fides of the bearer to those to whom they are presented, occasionally there will be challenges to that credential. This is particularly true during periods of heightened security. When such instances occur the following action will be taken:

- a. Bearer: Refer the authority that has questioned the credential to the phone number of the Program Manager.
- b. Command Center Watchstanders: If an identification query comes into the USCG Command Center, the responding watchstander will contact the appropriate Program Manager to verify the identity of the Credential bearer.

Note: Due to the sensitivity of the data contained in the Credential database, at no time will the verification authority, a Credentials Custodian, or a watchstander provide to the requesting agency the database access control to permit direct verification.

21. ENVIRONMENTAL ASPECTS AND IMPACT CONSIDERATIONS. Environmental considerations were examined in the development of this Instruction and have been determined to be not applicable.

22. FORMS AVAILALBILITY. None.

RDML R. S. Branham /s/
Assistant Commandant for Planning,
Resources and Procurement



AGENCY NAME - ALL CAPS
Times Bold - 20 pt centered/1!
linespacing
100% Cyan

NAME -
Times Bold - 17 pt centered
Black

TITLE -
Times Bold - 15 pt centered
Black



CB NUMBER -
Times Bold - 16 pt flush right
100% Cyan

PHOTOGRAPH -
Full Color - Front Facing
300dpi

TEXT -
Times - 7 pt justified
Linespacing - 7pt
Black

COAST GUARD BADGES AND CREDENTIALS PROGRAM

COMPLIANCE AUDIT PROCEDURES

1. Purpose: This enclosure outlines the requirements and procedures to be followed to accomplish the annual compliance audit for the USCG Badges and Credentials Program.
2. Responsibilities:
 - a. Office of Security Policy and Management, Commandant (CG-86):
 - (1) Establish an audit team to accomplish the annual oversight audit of CG Badges and Credentials Program.
 - (2) Establish an audit schedule that ensures the examination of all CG Badges and Credentials Programs each calendar year.
 - (3) Conduct Badges and Credentials Program audits in accordance with the guidelines, standards, and procedures outlined in this instruction and auditing best practices.
 - (4) Conduct follow-up inspections, as required, to ensure that audit deficiencies noted have been corrected.
 - b. Badges and Credentials Program Managers:
 - (1) Ensure that Credentials Custodians make available all program records for inspection by the audit team. Those records include but are not limited to: copies of references including this instruction, copies of the master inventory for credentials maintained, appointment letters for Credentials Custodians, implementation guidance for this instruction, documentation for required legal review, exemplars of materials used for production of credentials, destruction certificates (as appropriate), certifications for bearer eligibility/training, etc.
 - (2) Provide suitable workspace, communications and data base access for the audit team to facilitate audit conduct.
 - (3) Utilize the Self-Inspection checklist at Attachment 1 to prepare for the oversight audit.
3. Procedures: Badges and Credentials compliance audits will be accomplished as follows:
 - a. Notification: The Commandant (CG-86) audit team will forward via e-mail, or electronic message, a formal Notification of Audit seventy-two hours prior to the

- scheduled audit. That notification memo will outline team logistical and workspace requirements, and records and personnel access necessary to permit an accurate accounting of the program.
- b. Duration: Audits will normally not exceed one day in duration except in those instances where accountability problems are determined or the size of the program being examined is particularly large.
 - c. Schedule: Audits will include a short in-briefing for key personnel (Program Managers, Credentials Custodians and supporting staff), followed by the actual examination of material controls documents and interviews of key persons involved in the internal controls process. On completion of the audit examination, the Audit Team Chief will out-brief the Program Manager.
 - d. Scope: The compliance audit will focus on three broad areas of interest: Documentation (records and accountability), Supervision (Credentials Custodian appointment and actions), and Security (protection of data and materials).
 - e. Methodology: The audit team will utilize the checklist appended to this enclosure as its general outline. In addition, auditors will take a sample, verification testing, of the Badges and Credentials inventory for detailed validation of the effectiveness of controls. The size of this sample will be dependent on the size of the overall program, and in some cases may be 100% where the program is particularly small.
 - f. Findings: Audit reports will be prepared in the standard Findings and Recommendations format. Wherever practical, on site corrections may be accomplished and will not be included as report findings, but will be annotated as observations in the report.
4. Reports: Audit Reports will be forwarded to the Program Manager within 30 days of completion of the on-site phase of the audit. The audit team will prepare three copies of its final report. One copy will be provided to the Program Manager, one copy to Commandant (CG-86), and one copy to the ISLP.
5. Corrective actions: Audit respondents will accomplish corrective actions within 90 days of receipt of the audit report. They will prepare a Report of Corrective Actions addressing each finding and the corrective action accomplished. This report will be forwarded to Commandant (CG-86).

COAST GUARD BADGES AND CREDENTIALS PROGRAM

SELF-INSPECTION CHECKLIST

- Program Manager has published implementing guidance for U.S. Coast Guard Badges & Credentials Program.
- Program Manager has obtained legal review from G-L to ensure legal sufficiency of the authority that will be the focus of the program Credential.
- Program guidelines ensure that Credentials are only issued to Coast Guard Personnel (uniformed or civilian) or supporting contractors who have demonstrated requisite competence in the functional area for which they are required, and the maturity to judiciously exercise the authority specified in the credential.
- Individual bearer meets Program standards for credential issued and Program Manager maintains appropriate certification of training (formal schools or OJT) for credential qualification standards.
- Credential bearers have been briefed on the limits of the authority specified in the credential and what constitutes possible abuse of that authority.
- Credential Custodian appointed in writing, with name and contact data forwarded to Commandant (CG-86).
- Credential Custodian has properly secured and accounted for unused Credentials.
- Individual credentials are prepared utilizing DHS-approved serial numbered credential card stock, and in accordance with DHS design guidelines.
- Program Credentials Custodians issue credentials using a receipt system and log the issue data in their accountability database.
- Certificate of destruction for unserviceable Credentials is maintained by the custodian with the inventory records.
- Incident reports are provided to Commandant (CG-86) within 30 days when a Credential is reported stolen or missing.
- The Program Managers will maintain all Program Manager Letters of Certification, and records of retirement and destruction of Credentials as outlined in Schedule 18 of the General Records Schedule.
- Abuse of Credentials are investigated, an incident report prepared, and forwarded to Commandant (CG-86) within 30 days of completion.
- Commanders require bearers to turn in their Credentials as part of their mandatory unit out-processing procedures.