



Commandant  
United States Coast Guard

2703 Martin Luther King Jr. Ave SE  
Washington, DC 20593-7907  
Staff Symbol: CG-12  
Phone: (202) 475-5222

COMDTINST 12500.4  
09 OCTOBER 2019

COMMANDANT INSTRUCTION 12500.4

Subj: CYBERSECURITY EMPLOYEE RETENTION INCENTIVE PROGRAM

- Ref:
- (a) Title 5, United States Code, Section 5754
  - (b) Title 5, Code of Federal Regulations, Part 575, Subpart C
  - (c) DHS Cybersecurity Retention Incentive Plan, July 2017
  - (d) DHS Cybersecurity Workforce Coding Guidance, April 2016
  - (e) Cyberspace Operations Manual, COMDTINST M2620.2 (series)
  - (f) U.S. Coast Guard Competency Management System Manual, COMDTINST M5300.2 (series)
  - (g) Administrative Grievance Procedure, COMDTINST 12771.1 (series)

1. **PURPOSE.** This Instruction establishes Coast Guard policy and procedures governing the use of the Cybersecurity Employee Retention Plan for Coast Guard civilian employees paid from Operations and Support appropriations. The plan authorizes cybersecurity retention incentive payments for employees with critical cyber certifications or a group incentive payment for cybersecurity employees with unusually high or unique qualifications who are likely to leave Federal Service.
2. **ACTION.** All Coast Guard commanders, commanding officers, officers-in-charge, deputy commandants, assistant commandants, and HQ directors will comply with the provisions of this Instruction. Internet release is authorized.
3. **DIRECTIVES AFFECTED.** None.
4. **BACKGROUND.** DHS established the Cybersecurity Employee Retention Incentive Program to retain uniquely qualified employees in cybersecurity designated positions. References (a) through (c) authorizes DHS Components to develop a plan for using this incentive. Pursuant to the Department of Homeland Security (DHS) policies in References (c) and (d), this Instruction establishes the Coast Guard’s policy and procedures for using this incentive.

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	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X		X					
B	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
C	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
D	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X			X
E	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X	X	X				X	X		
F																	X	X	X	X						
G		X	X	X	X																					
H																										

NON-STANDARD DISTRIBUTION:

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 Instruction 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 Instruction 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 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 Instruction. An electronic version will be located on the following websites: <http://www.dcms.uscg.mil/directives> and CGPortal site: <https://cg.portal.uscg.mil/library/directives/SitePages/Home.aspx>.
8. PROCEDURES. Requests for cybersecurity retention incentive payments must be made in writing by the requesting official and endorsed by Commandant (CG-791). The request must be documented using (1) Cybersecurity Retention Incentive Request, Form CG-5305E, and (2) should include documentation that the employee is likely to leave Federal Service (a written job offer from an employer outside of the Federal government, justification letter from a supervisor, (3) or a component or office-level business case addressing market analysis and/or attrition rates supporting the need to pay a retention incentive, etc.). A request for an individual Cybersecurity Certification Incentive, should include the employee’s updated résumé and documentation of cybersecurity certification (s). A request for group cybersecurity certification should specify the unique qualifications and the names of each employee eligible to receive the group cybersecurity retention payment. Once endorsed by Commandant (CG-791), both an individual and a group request must be forwarded in FedHR to Commandant, (CG-123) for processing. After review and final approval by Commandant (CG-123), requests will be forwarded to Commandant (CG-832) for funds certification and tracking. The servicing Field or Center Human Resources Specialist will notify the employee of the final decision on the retention incentive request. Decisions made by Commandant (CG-123) or higher to deny or change the amount of a request shall not be appealed or grieved (5 C.F.R. 575.113 (5)(g)).

9. RECORDS MANAGEMENT CONSIDERATIONS. This Instruction has been evaluated for potential records management impacts. The development of this Instruction 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 (NARA) requirements, and the Information and Life Cycle Management Manual, COMDTINST M5212.12 (series). This policy does not have any significant or substantial change to existing records management requirements.
10. COVERAGE. This policy applies to appropriated fund permanent civilian employees in cyber designated positions including Senior Level, Scientific or Professional positions, and Senior Executive Service. Excluded positions can be found in Reference (c).
11. EQUAL OPPORTUNITY (EEO) STATEMENT. The Civilian employee cybersecurity retention incentive plan is free from unlawful discrimination and requests are considered without regard to race, color, national origin, religion, sex (including sexual orientation), age, disability, genetic information, marital status, parental status, political affiliation, engagement in a protected Equal Employment Opportunity (EEO) Activity, or any other basis protected by law.
12. GRIEVANCES. To determine appropriate grievance rights/procedures, consult Reference (g), for non-bargaining unit employees or the applicable negotiated agreements for bargaining unit employees. The receipt of or failure to receive a cybersecurity retention incentive is not grievable under Reference (g), which applies to all non-bargaining unit employees. In the case of bargaining unit employees, the negotiated grievance procedure of the applicable collective bargaining agreement must be followed as it pertains to whether the receipt of incentives and related issues are grievable.
13. POLICY. The Coast Guard may use an Individual Cybersecurity Retention Incentive and/or a Group Cybersecurity Retention Incentive to accomplish the Coast Guard's Cybersecurity mission and retain uniquely qualified employees. This policy aligns with the Department of Homeland Security Cybersecurity Retention Incentive Plan, Reference (c). In exercising this authority, responsible Coast Guard officials shall give due consideration to budgetary constraints as well as the Coast Guard's mission requirements.
14. CYBERSECURITY RETENTION INCENTIVES.
  - a. Identification of Retention Incentives.
    - (1) The DHS can identify one or more cybersecurity certifications in significant demand where it is likely employees will leave the Federal workforce.
    - (2) The Commandant (CG-791) may identify Coast Guard specific cybersecurity certifications for retention incentives not assigned by DHS.
  - b. Individual Cybersecurity Retention Incentive. The Coast Guard may pay a retention incentive of up to twenty-five (25) percent of basic pay to a current employee based on critical cybersecurity certifications that are in significant demand and necessary for

cybersecurity mission execution. The employee must possess a specific critical cybersecurity certification. The Coast Guard will determine:

- (1) If there is an unusually high or unique qualification or a special need for the employee's skills which makes it essential to retain the employee;
  - (2) If the employee would likely leave Federal Service in the absence of a retention incentive; and
  - (3) The basis for establishing the amount and timing of the approved retention incentive payment and the length of the required period.
- c. Group Cybersecurity Retention Incentive. The Coast Guard may pay a retention incentive of up to 10 percent of an employee's basic rate of pay for a group of cybersecurity employees with unusually high or unique qualifications essential to the Coast Guard and the Coast Guard determines there is a high risk a significant number of employees in the group would leave Federal Service in the absence of a retention incentive.
- d. Eligible employees may receive only one incentive, a group cybersecurity incentive or an individual cybersecurity incentive at same time as provided in 5 C.F.R. §575.209.

#### 15. DEFINITIONS.

- a. Individual Cybersecurity Retention Incentive is a retention incentive based on critical cybersecurity certifications that are in demand and necessary for the Department and the Coast Guard to execute its cybersecurity missions.
- b. Group Cybersecurity Retention Incentive is a retention incentive for a Coast Guard-designated group of cybersecurity employees with unusually high or unique qualifications who are likely to leave Federal Service.
- c. Requesting Official is a management or supervisory official (normally the immediate supervisor) who has the authority to make selections, and to propose final ratings of record for his/her subordinate employees.
- d. Rate of Basic Pay is the rate of pay fixed by law or administrative action for the position to which the employee is working in, before deductions and exclusive of additional pay of any kind. The rate of basic pay includes locality-based comparability payments or special pay adjustments.
- e. Cyber Workforce Coordinating Council (CWCC) establishes criteria and approves Department-wide certification-based retention incentives. It also conducts an annual review of the Department Cybersecurity Plan which includes a review of the Coast Guard's implementing policy.
- f. FedHR Navigator is the automated Civilian Human Resources Case Management System used by Coast Guard. Supervisors of civilian employees submit Cybersecurity Retention

Incentive Request, Form CG-5305E, with supporting documentation using FedHR Navigator. This system replaces paper and PDF versions of the Request for Personnel Action (SF-52).

- g. Cybersecurity Employee Retention Incentive Agreement means a written agreement between the Coast Guard and an employee under which the employee agrees to a specific period of employment and conditions with the agency in return for payment of a retention incentive.

16. CYBER DESIGNATED POSITION ELIGIBILITY CRITERIA. The following criteria shall be used to define eligible cybersecurity designated civilian positions.

- a. Positions coded in the National Finance Center payroll database as cybersecurity, and
- b. One of the following types of positions in accordance with 5 CFR §575.303:
  - (1) General Schedule (GS) or equivalent position;
  - (2) Senior level (SL) or scientific and professional position (ST);
  - (3) Senior Executive Service (SES) position (career appointee);
  - (4) Law enforcement officer position;
  - (5) Executive Schedule position or a position the rate of pay for which is fixed by law at a rate equal to a rate for the Executive Schedule;
  - (6) Prevailing rate position;
  - (7) Any other position in a category for which payment of retention incentives has been approved by DHS at the request of the head of an executive agency.

17. CIVILIAN EMPLOYEE ELIGIBILITY CRITERIA. To be eligible, civilian employees must:

- a. Have been employed by the Coast Guard on a permanent appointment for at least ninety (90) days;
- b. Currently encumber and is expected to remain in a designated cybersecurity position for the next twelve (12) months;
- c. Have not been demoted or suspended for performance or conduct reasons within the preceding 12 months; or, have not been issued a final decision for removal, demotion, or suspension after a finding by a deciding official;
- d. Have an overall rating of record of at least “Fully Successful,” “Meets,” or equivalent rating from another agency;

- e. Possess and maintain a current (non-expired) professional or industry certification that is related to the employee's position that is on the Department-wide list or the Coast Guard specific list of approved certifications; and
- f. Currently not receiving another cyber security incentive. Employees receiving a retention incentive under this Plan who change to another cybersecurity position in the Coast Guard (e.g., due to promotion, reassignment, detail etc.) before the expiration of the incentive term may be immediately eligible to receive an incentive in the new position if all other eligibility criteria are met.

18. RESPONSIBILITIES.

- a. The Office of Civilian Workforce Management (CG-122) has the following responsibilities:
  - (1) Develop, coordinate, and implement this Instruction and approve guidance for management.
  - (2) Develop and disseminate policies governing the use of the Cybersecurity Employee Retention Incentive Program and provide technical guidance to employing offices concerning its administration.
  - (3) Prepare requests through Commandant (CG-12) for retention incentives for career SES, SL, and ST positions, as limited by 5 C.F.R. §575.304 and submit to the DHS Under Secretary for final approval.
  - (4) Recommend approval or disapproval of requests to waive collection by Commandant (CG-8) and or DHS of a repayment debt in whole or in part, if it is determined that recovery would be against equity and good conscience or against the public interest.
  - (5) Evaluate on an annual basis the effectiveness of this incentive program. Prepare an annual retention incentive report to DHS, in conjunction with Commandant (CG-832), identifying the number of employees receiving incentives under this program, their job classifications, and the dollar amount of the incentives provided.
- b. The Office of Civilian Human Resources Operations (CG-123) has the following responsibilities:
  - (1) Maintain cybersecurity coding provided by Commandant (CG-791) in the National Finance Center database.
  - (2) Ensure that the required Cybersecurity Employee Retention Incentive Agreement has been signed by the employee and the Commandant (CG-123) supervisor.
  - (3) Use the Cybersecurity Retention Incentive Request, Form CG-5305E to verify eligibility and accuracy of information provided by requesting official.

- (4) Coordinate with Commandant (CG-124) to obtain appropriate clearance determination based on an individual's disciplinary, adverse and performance based actions or failure to meet a condition of employment.
  - (5) Provide final approval of cybersecurity employee retention requests prior to processing. Disapproved requests will be conveyed to the requesting official and will contain an explanation of the basis for the disapproval.
  - (6) Provide employees with the Cybersecurity Employee Retention Incentive Agreement based on approved requests for their signature. Inform employees of the proposed effective and/or termination dates of the incentives.
  - (7) Ensure Commandant (CG-832) certification of the availability of funds prior to authorizing payment.
  - (8) Process approved retention incentives, changes in incentive rates, and termination of incentives.
  - (9) Maintain a record of each determination made under this authority and retain the record for at least three years after the incentive has been paid. If the employee has not complied with the terms of his/her Cybersecurity Employee Retention Incentive Agreement, there are other disputes regarding the statement or the incentive payouts, or the incentive has become the subject of litigation, the records must be kept until the Coast Guard is notified by agency counsel that all pending claims have been resolved, all litigation concluded, and any applicable periods for seeking further review have elapsed, and in any event, for a minimum of six years from the date the facts giving rise to the dispute occurred. If debt collection is pursued against the employee for payments made by the Coast Guard, the Coast Guard must keep the records until notified by agency counsel that the debt is fully collected, compromised, or finally settled and that any applicable period for seeking further review has elapsed.
- c. Office of Cyberspace Forces (CG-791) has the following responsibilities:
- (1) Develop procedures for determining job-related cybersecurity certifications. Job related cybersecurity certifications will be documented in Reference (f).
  - (2) Determine coding for cybersecurity positions and provide the information to Commandant (CG-123).
  - (3) Determine whether a certification is required to perform the assigned cybersecurity work as documented in the Position Description or by an assigned competency in the Coast Guard Competency Management System.
  - (4) Publish, at least annually, a Cyber Operations Bulletin (COB) or ALCOAST/ACN that lists certifications, rates, and critical work roles for the group and individual incentives. Ensure the COB or ALCOAST/ACN will include the defining criteria for the group retention incentive. The COB or ALCOAST/ACN will be approved by Commandant (CG-7).

- (5) Review and endorse individual and group Cybersecurity Retention Incentive Requests, Form CG-5305E, in a fair and equitable manner. Submit all requests to Commandant (CG-123) using FedHR.
  - (6) Convey disapproved requests to the requesting official. Disapproved requests will contain the basis for the denial.
  - (7) Review, at least annually, each approved retention incentive, to determine whether it should be discontinued, continued, or terminated and reissued with new amount.
  - (8) Notify Commandant (CG-123) of any changes to eligible certifications, incentive rate changes, or when employee(s) are no longer eligible for a retention incentive.
  - (9) Provide data and estimates of expected number of personnel who will receive incentive payments in future years to Commandant (CG-832) and Commandant (CG-123).
- d. Commandant (CG-832) has the following responsibilities:
- (1) Review and certify each Cybersecurity Retention Incentive Request, Form CG-5305E for funding availability.
  - (2) Initiate collection procedures from the employee when appropriate; calculate the amount of any repayment due and, unless waived, ensure recoupment of any erroneous incentive payment money disbursed and is owed the Coast Guard.
  - (3) Prepare annual Cybersecurity Retention Incentive report for submission to Commandant (CG-122), identifying the number of employees receiving incentives under this Instruction based on actual pay records to include job series and the dollar amount paid.
  - (4) Manage prior, current, and future years' account balances.
  - (5) Provide a list of retention incentive transactions (unliquidated obligations) for review and validation for continuance.
  - (6) Monitor and analyze budget execution patterns and ensure that funds are obligated in a timely manner, in accordance with applicable law, and in harmony with program priorities.
  - (7) After receiving input from Commandant (CG-791), forecast future year costs and formulate the Cybersecurity Employee Retention Incentive budget limits.
- e. Supervisors of Cybersecurity Employees have the following responsibilities:
- (1) Document any request for a Cybersecurity Retention Employee Incentive by completing the Request for Cybersecurity Employee Retention Incentive.



- (2) Prepare a written request to include an email certification from management that the employee is seeking employment opportunities outside the Federal government or the employee is in receipt of a job offer, or a market analysis and/or attrition rate supporting the potential for a retention incentive for an employee (or groups of employees).
  - (3) Provide documentation of job-related cybersecurity certifications to include, expiration dates, issuing/credentialing entity, name and contact information, and any other relevant information determined by the CWCC or Coast Guard.
  - (4) Provide documentation (e.g., Standard Form SF-52, position description annotated with cyber certification) in the automated system of record (e.g., FedHR) to Commandant (CG-123) for details within and outside of the Coast Guard for longer than 30 days. The supervisor should include a statement indicating the Coast Guard should continue or discontinue payment of the employee's Cybersecurity retention incentive (s) using a short description of the duties to be performed during the detail.
  - (5) Track and ensure employee's cyber certifications are current and notify Commandant (CG-791) and servicing Field or Center HR Specialist if certification expires.
  - (6) Use Cybersecurity Retention Incentive Request, Form CG-5305E to request an individual or group cybersecurity retention incentive, if eligibility criteria are met.
  - (7) Endorse the request and submit it with supporting documentation, if the request meets program compliance. The request is sent to Commandant (CG-791) for authorization and submission to Commandant (CG-123) for final approval.
  - (8) Provide the signed Cybersecurity Employee Retention Incentive Agreement to the Field or Center HR Specialist.
  - (9) Immediately report any employee eligibility changes (including projected loss of certifications, and suspension or revocation of security clearances, if applicable) made after the end of the approval period to Commandant (CG-791) and servicing Field or Center HR Specialist.
  - (10) Notify Commandant (CG-791) and servicing Field or Center HR Specialist office when an employee is leaving their current cybersecurity position (e.g. due to promotion reassignment, etc.).
  - (11) Notify Commandant (CG-791) and servicing Field or Center HR Specialist prior to detailing an employee receiving a cybersecurity retention incentive.
- f. Employees who are seeking this incentive have the following responsibilities:
- (1) Provide to their supervisors documentation of job-related cybersecurity certifications which includes: expiration dates, issuing/credentialing entity, name and contact information and any other relevant information determined as necessary by the CWCC or Coast Guard.

- (2) Inform their supervisors if they are interested in seeking employment opportunities outside of the Federal government. Employees shall also seek guidance from their servicing legal office if their desired post-government employment may conflict with their current or former Federal duties, as governed by 5 C.F.R. Part 2641.
  - (3) Maintain each certification in accordance with issuing authority guidelines.
  - (4) Meet recertification requirements and deadlines while receiving a certification-based retention incentive.
  - (5) Immediately report any change in eligibility (including projected loss of certifications, and suspension or revocation of their security clearance, if applicable) for a retention incentive and any additional retention incentive payments made after the end of the approval period to their supervisors. In the event an employee incurs a debt, they will be responsible to repay any incentives erroneously received.
  - (6) Understand if there is no other independent basis for the certification or category incentive, the retention incentive will be terminated in accordance with the Cybersecurity Employee Retention Incentive Agreement.
  - (7) Understand if certifications expire and/or they fail to provide updated certifications to their supervisors; they are ineligible to continue to receive cybersecurity retention incentive payments. In accordance with the Cybersecurity Employee Retention Incentive Agreement, the employee are responsible to notify their supervisors and must repay incentives erroneously paid in excess of the sums agreed upon in this agreement.
  - (8) Notify their supervisors when leaving their current cybersecurity position (e.g. due to promotion, reassignment, etc.). In the event an employee incurs a debt, they will be responsible to repay any incentives erroneously received.
  - (9) Notify their supervisors prior to any detail assignment during the period they are receiving a cybersecurity retention incentive payment. In the event an employee incurs a debt, they will be responsible to repay any incentives erroneously received.
  - (10) Once the Cyber Retention Incentive Request is approved and the employee agrees to enter into the Cybersecurity Employee Retention Incentive Agreement, the employee and a Coast Guard representative have to sign the Cybersecurity Employee Retention Incentive Agreement and provide it to their supervisor.
19. **REQUIRED FUNDING.** Assistant Commandant for Resources (CG-8) will promptly make final funding determinations, subject to the availability of funds. Local funds will not be used to fund this program.
20. **AGGREGATE INCENTIVE LIMITATION.** An employee may not receive an incentive, differential, bonus, award, or similar payment in combination with basic pay which would exceed Level I of the Executive Schedule, as limited by 5 C.F.R. Part 530, Subpart B.

21. CRITERIA FOR PAYING INCENTIVES. The determination that a retention incentive, and the amount of that retention incentive, is appropriate shall be based on written documentation and following factors listed in 5 C.F.R. § 575.306 (b) and (c):

- a. The specific job-related cybersecurity certification for which the CWCC or Coast Guard has determined that a retention incentive is warranted and the rate associated with the certification.
- b. The success of recent efforts to recruit candidates and retain employees with qualifications similar to those possessed by the employee for positions similar to the position held by the employee.
- c. The unusually high or unique qualifications of the employee (or group of employees) or a special need of the agency for the employee's (or group of employees') services makes it essential to retain the employee(s);
- d. The employee (or a significant number of employees in a group) would be likely to leave the Federal Service in the absence of a retention incentive; and
- e. The amount and timing of the approved retention incentive payment and the length of the required service period.

22. METHOD AND CONDITIONS OF PAYMENT. The payment of Cybersecurity Employee Retention Incentives will be made and reviewed in the follow manner:

- a. A retention incentive will be paid in biweekly installment payments at the full retention incentive percentage approved for the employee or group for NTE 26 pay periods beginning the first full pay period after approval by Commandant (CG-123) and the date the employee's Cybersecurity Employee Retention Incentive Agreement is signed by the employee and Coast Guard representative.
- b. The payment period begins on the effective date of the personnel action.
- c. An employee who, voluntarily or due to unsatisfactory performance or misconduct, fails to meet the provisions of the Agreement, may retain all payments previously made to the employee that are attributable to completed service, but is not entitled to, and will not receive, any additional amount for future payments.
- d. Extensions or increases to incentive payments require submission of a new request. Requests for continuation shall be submitted via the Cybersecurity Retention Incentive Request, Form CG-5305E and address the same requirements as for original approval. The approval level remains the same as specified in Paragraph 8. Extensions or increases must be submitted to Commandant (CG-123) at least 45 days before the expiration of the current Cybersecurity Employee Retention Incentive Agreement.
- e. Cybersecurity retention payments can continue under the terms of the Agreement during minor lapses (i.e. less than 90 days) in certification due to events beyond the employee's control as determined by Commandant (CG-123).

23. TERMINATION OF CYBERSECURITY RETENTION INCENTIVE. An employee receiving cybersecurity retention incentive payments will be ineligible for continued payments if he/she:

- a. Separates from the Coast Guard for any reason;
- b. Is demoted for cause;
- c. Fails to maintain at least a “Meets” (for employees under the Excellence, Achievement, and Recognition performance system), an “Achieved Expectations” (for employees under the DHS Performance Management Program) level of performance, or a “Minimally Satisfactory” (for employees under the Senior Executive Service Performance Management System);
- d. Fails to maintain cyber certifications;
- e. Violates any of the conditions of the Cybersecurity Employee Retention Incentive Agreement.
- f. Fails to meet a condition of employment.

24. CYBERSECURITY EMPLOYEE RETENTION INCENTIVE AGREEMENT.

- a. Before a retention incentive is approved, a Cybersecurity Employee Retention Incentive Agreement must be signed by the employee and a Coast Guard representative. The Cybersecurity Employee Retention Incentive Agreement is executed for a specific position; the employee's subsequent movement into a different position could terminate payments.
- b. The Cybersecurity Employee Retention Incentive Agreement in no way constitutes a right, promise, or entitlement to a perpetual retention incentive, continued employment; or non-competitive conversion to the competitive service, nor does it limit management's right to take disciplinary, adverse, or performance based action as appropriate.

25. RECORDS RETENTION. Commandants (CG-123) and (CG-791) will maintain records of individual and group cybersecurity retention incentive requests, decisions, and agreements in a secure filing system for three years after the effective date of the incentive or as defined in Paragraph 18.b.(9) of this Instruction.

26. FORMS.REPORTS. None.

27. REQUEST FOR CHANGES. Recommendations for improvements to the Cybersecurity Civilian Employee Retention Incentive Program should be submitted to Commandant (CG-122) through the chain of command.

MICHELLE R. GODFREY /s/  
Director, Civilian Human Resources,  
Diversity, and Leadership

Encl: (1) Cybersecurity Retention Incentive Request, Form CG-5305E

THIS PAGE IS INTENTIONALLY LEFT BLANK

DEPARTMENT OF HOMELAND SECURITY  
U.S. Coast Guard  
**CYBERSECURITY RETENTION INCENTIVE REQUEST**

General Instructions: *Parts 1 and 3 should be completed by the original requestor (supervisor) with the assistance and coordination of the Field or Servicing Human Resources Specialist. Employees and the Coast Guard representative must sign the Cybersecurity Retention Employee Incentive Agreement before payments can begin.*

**Part 1: Basic Information about the Request**

This request is for the Cybersecurity Retention Incentive, pursuant to COMDTINST 12500.4:

A cybersecurity retention incentive of \_\_\_\_\_ (percent of locality pay) \_\_\_\_\_ (indicate biweekly dollar amount) for \_\_\_\_\_ (number of pay periods, not to exceed twenty six (26) without reapproval).

Complete the following information about the employee:

Name of Employee \_\_\_\_\_

(If for a group retention allowance, specify in Part 3 the criteria for group identification and name all individual members; additional members may be added by memorandum signed by the responsible program director)

Title, Pay Plan, Series, Grade, Step, and Locality Salary \_\_\_\_\_

Organization and Location \_\_\_\_\_

Prospective Pay of Job Offer Salary (if the employee is leaving Federal service) \_\_\_\_\_

A. For individual cybersecurity retention incentives:

1. Specify the current cybersecurity certifications the employee holds, including expiration dates (attach copies with the request):
2. Attach a copy of the employee's current résumé, the job application, and/or job offer (if available) to the request.

B. For group cybersecurity retention incentives:

1. Identify the name of each employee eligible for the group incentive.

**Part 2: Request and Approval Signatures**

Organization	Approve	Disapprove	Date
Requestor			
CG-791			
CG-123			
CG-8362			
CG-12 (for SES, SL/ST positions for submission to DHS)			

**PRIVACY NOTICE**

**AUTHORITY:** 5 U.S.C. § 5754

**PURPOSE:** To determine if a United States Coast Guard (USCG) civilian employee meets service eligibility for a general bonus.

**ROUTINE USES:** Authorized USCG officials will use this information to determine if a USCG employee meets service eligibility criteria for a general bonus. DHS/USCG-014, Military Pay and Personnel, October 28, 2011, 76 Federal Register 66933 provides coverage for this collection.

**DISCLOSURE:** Providing this information is voluntary. However, failure to provide this information may result in a delay in processing this agreement.

DEPARTMENT OF HOMELAND SECURITY  
U.S. Coast Guard  
**CYBERSECURITY RETENTION INCENTIVE REQUEST**

**Part 3. a. Justification Criteria.** Provide a written justification on page 3 that meets the criteria specified below. Consult with your Field or Servicing Human Resources Specialist and submit the request and accompanying documentation through the FedHR system to your field or servicing Human Resources Specialist.

Justification for a Cybersecurity Retention Incentive.

Demonstrate:

- 1) That the nominated employee has an unusually high or unique qualification or that there is a special need for the employee's skills which makes it essential to retain the employee;
- 2) That absent an incentive, the employee is likely to leave Federal service (a written job offer from an employer outside of the Federal Service, justification letter from a senior level management official, or a component or office-level business case addressing market analysis and/or attrition rates supporting the need to pay a retention incentive);
- 3) The extent to which the employee's departure would affect the Coast Guard's ability to carry out an activity or perform an essential cyber security function (identify other employees at the command who occupy similar positions or perform similar functions and demonstrate the special uniqueness or conditions that apply to the individual for whom the allowance is requested);
- 4) The success of recent efforts to recruit candidates and retain employees with qualifications similar to those possessed by the employee for positions similar to those held by the employee;
- 5) The availability in the labor market of candidates for employment who, with minimal training or disruption of service to the public, could perform the full range of duties and responsibilities assigned to the position held by this employee.
- 6) If the retention allowance is for a group, specify the criteria for identifying the group and name the individual members. Demonstrate (1) the unusually high or unique qualifications or special need to retain the employees and (2) there is a high risk a significant number may leave Federal service based on evidence of extreme labor market conditions, high private sector demand, or Federal/private sector disparities in salaries.

Civilian Employees Eligibility Criteria. To be eligible, civilian employees must:

- 1) Have been employed by the Coast Guard on a permanent appointment for at least ninety (90) days;
- 2) Currently encumber and expected to remain in a designated cybersecurity position for the next twelve (12) months;
- 3) Have not been demoted or suspended for performance or conduct reasons within the preceding 12 months; or, have not been issued a final decision for removal, demotion, or suspension after a finding by a deciding official;
- 4) Have an overall rating of record of at least "Fully Successful," "Meets," or equivalent rating from another agency;
- 5) For certification-based incentives, possess and maintain a current (non-expired) professional or industry certification that is related to the employee's position that is on the Department-wide list or the Coast Guard specific list of approved certifications.
- 6) Terminate current cybersecurity retention incentive agreement prior to receiving another incentive



DEPARTMENT OF HOMELAND SECURITY  
U.S. Coast Guard  
**CYBERSECURITY RETENTION INCENTIVE REQUEST**

**Part 3.b. Written Justification.** Use this page to justify the request against the criteria specified in Part 3.a.