U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Office of the Director
Washington, DC 20528

August 18, 2021

SENT VIA EMAIL TO: foia@americanoversight.org

Mehreen Rasheed
American Oversight
1030 15th Street, NW
Suite B255
Washington, DC 20005

RE: CISA Case Number 2021-NPFO-00011

Dear Mr. Rasheed:

This letter is the final response to your Freedom of Information Act (FOIA) request to U.S. Department of Homeland Security (DHS), Cybersecurity & Infrastructure Security Agency (CISA) dated November 19, 2020. You have requested all formal letters or memoranda written or signed by CISA Director Chris Krebs or Deputy Director Matt Travis from November 3, 2020, through November 17, 2020. CISA has considered your request under the FOIA, 5 U.S.C. § 552.

A search of CISA for records produced 69 pages that are responsive to your request. Following review, CISA has determined that portions these pages will be withheld pursuant to Exemptions (b)(5), (b)(6), and (b)(7)(E) of the FOIA as described below.

Enclosed are 69 pages with certain information withheld as described below:

FOIA Exemption 5 protects from disclosure those inter- or intra-agency documents that are normally privileged in the civil discovery context. The three most frequently invoked privileges are the deliberative process privilege, the attorney work-product privilege, and the attorney-client privilege. After carefully reviewing the responsive documents, we determined that portions of the responsive documents qualify for protection under the Deliberative Process Privilege**.** The deliberative process privilege protects the integrity of the deliberative or decision-making processes within the agency by exempting from mandatory disclosure opinions, conclusions, and recommendations included within inter-agency or intra-agency memoranda or letters. The release of this internal information would discourage the expression of candid opinions and inhibit the free and frank exchange of information among agency personnel.

FOIA Exemption 6 exempts from disclosure personnel or medical files and similar files the release of which would cause a clearly unwarranted invasion of personal privacy. This requires a balancing of the public's right to disclosure against the individual's right to privacy. The privacy

interests of the individuals in the records you have requested outweigh any minimal public interest in disclosure of the information. Any private interest you may have in that information does not factor into the aforementioned balancing test.

Exemption 7(E) protects records compiled for law enforcement purposes, the release of which would disclose techniques and/or procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law. I determined that disclosure of law enforcement information could reasonably be expected to risk circumvention of the law. Additionally, the techniques and procedures at issue are not well known to the public.

You have a right to appeal the above withholding determination. Should you wish to do so, you must send your appeal and a copy of this letter, within 90 days of the date of this letter, to: Privacy Office, Attn: FOIA Appeals, U.S. Department of Homeland Security, 245 Murray Lane, SW, Mail Stop 0655, Washington, D.C. 20528-0655, following the procedures outlined in the DHS FOIA regulations at 6 C.F.R. Part 5 § 5.8. Your envelope and letter should be marked "FOIA Appeal." Copies of the FOIA and DHS FOIA regulations are available at www.dhs.gov/foia.

Provisions of FOIA allow DHS to charge for processing fees, up to $25, unless you seek a waiver of fees. In this instance, because the cost is below the $25 minimum, there is no charge.

You may send an e-mail to foia@hq.dhs.gov, call 202-343-1743 or toll free 1-866-431-0486, or you may contact our FOIA Public Liaison in the same manner. Additionally, you have a right to right to seek dispute resolution services from the Office of Government Information Services (OGIS) which mediates disputes between FOIA requesters and Federal agencies as a non-exclusive alternative to litigation. If you are requesting access to your own records (which is considered a Privacy Act request), you should know that OGIS does not have the authority to handle requests made under the Privacy Act of 1974. You may contact OGIS as follows: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, Maryland 20740-6001, e-mail at ogis@nara.gov; telephone at 202-741-5770; toll free at 1-877-684-6448; or facsimile at 202-741-5769.

If you need to contact our office again about this matter, please refer to FOIA case number 2021-NPFO-00011. This office can be reached at FOIA@hq.dhs.gov.

Sincerely,

Jimmy Wolfrey

Jimmy Wolfrey
Senior Director, FOIA Operations and Management
(Acting)

Enclosures: 69 pages

If you are not satisfied with the response to this request, you may administratively appeal. Should you wish to do so, you must send your appeal and a copy of this letter, within 90 days of the date of this letter, to: Privacy Office, Attn: FOIA Appeals, U.S. Department of Homeland Security, 245 Murray Lane, SW, Mail Stop 0655, Washington, D.C. 20528-0655 or email to foia@hq.dhs.gov, following the procedures outlined in the DHS FOIA regulations at 6 C.F.R. Part 5 § 5.8. Your envelope and letter should be marked "FOIA Appeal." Copies of the FOIA and DHS FOIA regulations are available at www.dhs.gov/foia.

Provisions of FOIA allow DHS to charge for processing fees, up to $25, unless you seek a waiver of fees. In this instance, because the cost is below the $25 minimum, there is no charge.

You may contact the CISA FOIA Public Liaison at 703-235-2211 for any further assistance and to discuss any aspect of your request. Additionally, you have a right to right to seek dispute resolution services from the Office of Government Information Services (OGIS) which mediates disputes between FOIA requesters and Federal agencies as a non-exclusive alternative to litigation. If you are requesting access to your own records (which is considered a Privacy Act request), you should know that OGIS does not have the authority to handle requests made under the Privacy Act of 1974. You may contact OGIS as follows: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, Maryland 20740-6001, e-mail at ogis@nara.gov; telephone at 202-741-5770; toll free at 1-877-684-6448; or facsimile at 202-741-5769.

If you need to contact our office again about this matter, please refer to FOIA case number **2021-NPFO-00011**. This office can be reached at CISAFOIA@HQ.DHS.GOV or at 703-235-2211.

Enclosure(s): 69 page(s)

U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Integrated Operations Division
Washington, DC 20528

October 15, 2020

DECISION

MEMORANDUM FOR THE DIRECTOR

THROUGH: Emily Early
Chief of Staff

(b)(6)

THROUGH: Richard Driggers
Assistant Director

FROM: David Wilkinson
Deputy Associate Director, CISA Central

(b)(6)

SUBJECT: (b)(5)

(b)(6); (b)(5)

(b)(6); (b)(5)

(b)(5)

NOV 5 2020

(b)(6)

Approve/date

Disapprove/date_____

Modify/date _____

Needs discussion/date_____

Attachment:

1. (b)(5)

U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Office of the Director
Washington, DC 20528

November 5, 2020

DECISION

MEMORANDUM FOR THE DEPUTY UNDER SECRETARY FOR MANAGEMENT

FROM: Christopher C. Krebs
Director (b)(6)

SUBJECT: (b)(5)

(b)(6); (b)(5)

(b)(5)

Approve/date_____ Disapprove/date_____

Modify/date _____ Needs discussion/date_____

Attachments:

(b)(5)

U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Stakeholder Engagement Division
Washington, DC 20528

August 26, 2020

DECISION

MEMORANDUM FOR THE DEPUTY DIRECTOR

THROUGH: Bradford Willke
Acting Assistant Director
(b)(6)

FROM: Bradford Tenney
Assistant Chief of Staff
(b)(6)

SUBJECT: (b)(5)

(b)(5)

(b)(6); (b)(5)

(b)(5)

(b)(6)

Approve/dat NOV2020 Disapprove/date_____

Modify/date _____ Needs discussion/date_____

U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Office of the Director
Washington, DC 20528

November 6, 2020

MEMORANDUM FOR DISTRIBUTION

(b)(6)

FROM: Matthew Travis
Deputy Director

SUBJECT: **Action: Integrated and Unified Stakeholder Relationship Information Management; Next Steps**

Purpose: This memorandum establishes the next set of deliverables for the Integrated and Unified Stakeholder Relationship Information Management initiative, established in a Memorandum for Distribution Action released on January 29, 2020.

Context: The previous memorandum established the Stakeholder Engagement and Cyber Infrastructure Resilience (SECIR) Division as the steward for the Stakeholder Relationship Management (SRM) program and its associated technology platform. As the successor organization to SECIR, the Stakeholder Engagement Division (SED) assumes this role and stewardship and leads the SRM Task Force.

In its first 120 days, the task force has delivered the following:

1. SRM Task Force Charter
2. SRM project plan
3. Initial and monthly reports including issues and obstacles with recommendations for mitigation
4. Initial and final agency-wide business requirements
5. Initial and final agency-wide use cases
6. SRM prototype user testing and feedback on schedule

The SRM Task Force has recommended that it continues to facilitate a cross-Cyber Security and Infrastructure Security Agency (CISA) collaborative approach to develop the next set of deliverables.

Directed Actions: To continue the progress of this initiative, I direct the next set of actions to implement this program:

1. The SRM Task Force remains active and takes responsibility for helping the SRM Program achieve final operating capability (FOC) by December 2020. The task force submits to me, via SED, a monthly report detailing the status of deliverables, participation records, and a list of issues, obstacles, and recommendations for resolution as needed to assure "fast-track" progress on this initiative.

2. The task force provides deliverables for this initiative on the following schedule:

Days from memo issuance	SRM Task Force Deliverables
30 days	1. Updated SRM Project Plan, to include task force milestones, deliverables, and resources needed to reach FOC by December 2020. 2. Listing of all needed SRM Task Force working groups to include roles and responsibilities.
60 days	1. SRM user testing and feedback results. 2. Updated CISA-wide use cases to include addressing user testing feedback, following the Agile process.
90 days	1. Completed draft for initial SRM Concept of Operations. 2. SRM Initial Operating Capability user testing and feedback results. 3. Draft User Adoption Plan to include validated user count for SRM Fiscal Year 2021 for licensing and training. 4. Updated CISA-wide use cases to include addressing user testing feedback, following the Agile process.
120 days	1. Resolved flagged SRM items, including those for data governance and for official use only (FOUO) security. 2. SRM FOC user testing and feedback. 3. Updated CISA-wide use cases to include addressing user testing feedback, following the Agile process. 4. SRM data dictionary. 5. Final End-user Adoption Plan. 6. Training guides. 7. Draft SRM Directive. 8. List of remaining CISA-wide use cases for post-FOC development.
150 days	1. SRM FOC implementation summary report and lessons learned. 2. SRM Standards and User Guide. 3. SRM Concept of Operations.

3. SED provides the following deliverables in parallel with the work of the SRM Task Force by the end of calendar year 2020:
   a. Final SRM Directive
   b. SRM Lifecycle Management Plan
   c. SRM Knowledge Management Strategy
   d. SRM Operating Manual
   e. Establishment of Help Desk

Successful implementation of this function is a key outcome of *CISA 2020,* and I will maintain visibility of its progress. Issues are to be escalated to me as required. I ask for your support in establishing this essential new capability for CISA.

SED has designated (b)(6) as the lead for this initiative and will be relying on the task force to complete all deliverables.

Distribution:

Chief of Staff
Executive Director
Assistant Director for Cybersecurity
Assistant Director for Infrastructure Security
Assistant Director for Emergency Communications
Assistant Director for National Risk Management Center
Assistant Director for Stakeholder Engagement
Assistant Director for Integrated Operations
Chief of Strategy, Policy, and Plans
Chief External Affairs Officer
Chief Counsel
Chief Human Capital Officer
Chief Financial Officer
Chief Operations Support Officer
Chief Information Officer
Chief Technology Officer
Chief Information Security Officer
Chief Security Officer
Chief Acquisition Executive
Chief Privacy Officer
Chief of Workforce Engagement
Chief of Contracting Officer
Chief Learning Officer
Equal Employment Opportunity Officer
Regional Director – Region 1
Regional Director – Region 2
Regional Director – Region 3
Regional Director – Region 4
Regional Director – Region 5
Regional Director – Region 6
Regional Director – Region 7
Regional Director – Region 8
Regional Director – Region 9
Regional Director – Region 10

U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Office of the Chief Operations Support Officer
Washington, DC 20528

October 9, 2020

DECISION

MEMORANDUM FOR THE DIRECTOR

FROM: Nicole Windham
Chief Operations Support Officer

(b)(6)

SUBJECT: (b)(5)

(b)(5)

(b)(6); (b)(5)

(b)(5)

NOV 5 2020

(b)(6)

Approve/date Disapprove/date_____

Modify/date _____ Needs discussion/date_____

U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Office of the Director
Washington, DC 20528

November 5, 2020

MEMORANDUM FOR DISTRIBUTION

FROM: Christopher C. Krebs
Director

(b)(6)

SUBJECT: **Policy Statement: Cybersecurity and Infrastructure Security Agency Transportation Service Program**

Purpose: The purpose of this memorandum is to establish the Cybersecurity and Infrastructure Security Agency (CISA) Transportation Service (CTS) Program, which provides transportation services to authorized CISA federal employees between locations throughout the National Capital Region (NCR) to conduct official government business.

Context: CISA supports the Department of Homeland Security (DHS) mission to protect our Nation by leading the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure. CISA consists of the Director's Office, Mission Support Offices, the Cybersecurity Division, the Emergency Communications Division, the Infrastructure Security Division, the Integrated Operations Division, the Stakeholder Engagement Division, and the National Risk Management Center, all of which are headquartered within the NCR.

CISA's mission requires its employees within these divisions and offices to physically attend briefings, meetings, and other engagements with congressional staff and committees, inter and intra-department counterparts, and public stakeholders at various locations within the NCR. For the purposes of this memorandum and its attachments, the NCR includes the area within a 50-mile radius of 1110 North Glebe Road, Arlington, Virginia (VA). These meetings are often held at locations where public transportation or parking are not readily available. Meetings are also often scheduled at certain locations, frequencies and times where the use of public transportation is impractical or inefficient.

The Office of the Chief Operations Support Officer (OCOSO) establishes and administers the CTS Program, which is provided under an intra-agency agreement with the Immigration and Customs Enforcement (ICE) agency. The CTS delivers authorized CISA federal employees predictable and schedulable point-to-point passenger transportation services within the NCR via sedan or van service, based on passenger requirements (e.g., group size). This allows employees to travel efficiently between various locations during their official government duties. The previous transportation service provided through an agreement with DHS Headquarters was limited to supporting a fraction of CISA executives. This agreement with ICE ensures broader and more reliable coverage of official business transportation requirements open to all CISA employees.

Policy Statement: The CTS Program is established to provide transportation services to CISA federal employees within the NCR to efficiently conduct official business.

1. This service is open to eligible CISA federal staff based in the NCR, not those traveling to the NCR on official business.
2. This policy is authorized by numerous laws, regulations, and policies including, but not limited to:
    a. 31 United States Code (U.S.C.) 1344, "Passenger Carrier Use"
    b. 31 U.S.C. 1349, "Adverse Personnel Actions"
3. Pursuant to the aforementioned authorities, the OCOSO exercises executive oversight of the program to ensure sufficient resources are available to execute the CTS Program. The program is set up as follows:
    a. CISA employees submit reservation requests via the CTS Request Template available on the CISA Point Logistics webpage.
    b. The service is available within a 50-mile radius from 1110 North Glebe Road, Arlington, VA (see attached CISA Transportation Service Program Map).
    c. Additional information about eligibility requirements, request procedures, and hours of operation are in the attached CTS Program Desk Aid.
4. All users of the CTS are responsible for requesting service and following the guidance outlined in this policy and the attached CTS Program Desk Aid. Requesters or users who do not provide required information or do not comply with the requirements outlined in this policy may experience delayed service or may be denied service.

    All CISA employees using or authorizing the use of government-owned or controlled vehicles are to be aware that such vehicles can be used only for official government business and that use otherwise is contrary to law. Employees using, requesting, or authorizing requests to use the CTS are to be aware that use is subject to audit. By requesting, confirming official business purposes, and using the CTS, the requester and the authorized user confirm understanding of the relevant authorities and the requirements for use established in this policy.
5. This policy is effective immediately.

The CISA lead point of contact for this policy is Associate Chief for Logistics, (b)(6) (b)(6)

Duration: This policy remains in effect until it is replaced with a directive, an updated policy statement, or rescinded.

Attachments:
1. CISA Transportation Service Program Map
2. CTS Program Desk Aid

Distribution:

CISA-ALL

U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Integrated Operations Division
Washington, DC 20528

September 17, 2020

DECISION

MEMORANDUM FOR THE DIREC[redacted] (b)(6)

FROM: John Felker
Assistant Director

SUBJECT: (b)(5) [redacted]

(b)(5) [redacted]

(b)(6); (b)(5)

(b)(6); (b)(5)

NOV 17 2020

Approve/date (b)(6)

Disapprove/date_____

Modify/date _____

Needs discussion/date_____

U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Stakeholder Engagement Division
Washington, DC 20528

November 3, 2020

DECISION

MEMORANDUM FOR THE DIRECTOR

FROM: Bradford Willke
(Acting) Assistant Director (b)(6)

SUBJECT: (b)(5)

(b)(6); (b)(5)

(b)(5)

Recommendation: (b)(6); (b)(5)

Approve/date (b)(6) **11/16/2020** Disapprove/date _____

Modify/date _____ Needs discussion/date _____

Attachment(s):

(b)(5)

U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Office of the Chief Human Capital Officer
Washington, DC 20528

September 21, 2020

DECISION

MEMORANDUM FOR THE DIRECTOR

FROM: Rita J. Moss
Chief Human Capital Officer (b)(6)

SUBJECT: (b)(5)

(b)(6); (b)(5)

(b)(5)

(b)(5)

NOV 5 2020

Approve/dat (b)(6) Disapprove/date_____

Modify/date _____ Needs discussion/date_____

U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Cybersecurity Division
Washington, DC 20528

October 8, 2020

DECISION

MEMORANDUM FOR THE DIRECTOR

FROM: Bryan Ware
Assistant Director
(b)(6)

SUBJECT: (b)(5)

(b)(6); (b)(5)

(b)(6)

(b)(6); (b)(5)

NOV 16 2020

Approve/date (b)(6) Disapprove/date_____

Modify/date _____ Needs discussion/date_____

Attachments:
1. MOA USCG to CSD (b)(6) June2019_signed
2. MOA Addendum_DHS_CISA_CSD with USCG (b)(6)
3. Letter to USCG from Director Krebs

U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Office of the Director
Washington, DC 20528

November 16, 2020

Admiral Karl Schultz
Commandant
U.S. Coast Guard
2703 Martin Luther King Jr., S.E.
Washington, District of Columbia 20593

Dear Admiral Schultz,

I write to you to extend my deepest appreciation of the Coast Guard members detailed to the Cybersecurity and Infrastructure Security Agency (CISA). CISA has over 20 active duty Coast Guard members assigned to the Cybersecurity Division (CSD) and their diverse portfolio of expertise and contributions to CISA have truly been remarkable. One Coast Guard detailee—Commander (sel.) (b)(6) —is assigned concurrently to both the Strategy, Performance, and Resources (SPR) sub-division and the Cyber Defense Education and Training (CDET) sub-division.

(b)(6) has certainly stood out while on detail at CISA, as she has brought unique talents to our evolving workforce. She has embodied what it means to be "One CISA" and her contributions have centered on one of my six core governance principles of equity and inclusiveness with our Agency stakeholders. Within SPR, she continues to be a driving force behind the cross-divisional Industrial Control Systems (ICS) Operating Committee, which has enabled this group of subject matter experts to be on the forefront of anticipating, prioritizing, and managing national-level ICS risk. (b)(6) is also an active member of the CISA-led Control Systems Interagency Working Group to develop national-level plans and policy concerning incident management, workforce development, supply chain risk management, and standards for operational technology within U.S. critical infrastructure. Lastly, (b)(6) is the intellectual powerhouse behind the development of our CDET Engagement Strategy. As evidence to the positive reach and impact she has already made at CISA, this strategy will enable us to strengthen and forge new partnerships designed to systematically address the national cybersecurity workforce shortage, where the Coast Guard's cyber workforce will also benefit. She continues to bolster key relationships between CISA and the Coast Guard.

Given the unique talents of (b)(6) it is unquestionably essential to extend her current detail with CISA for an additional 2 years through June 2023.

Sincerely,

(b)(6)

Christopher C. Krebs
Director

U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Stakeholder Engagement Division
Washington, DC 20528

October 13, 2020

DECISION

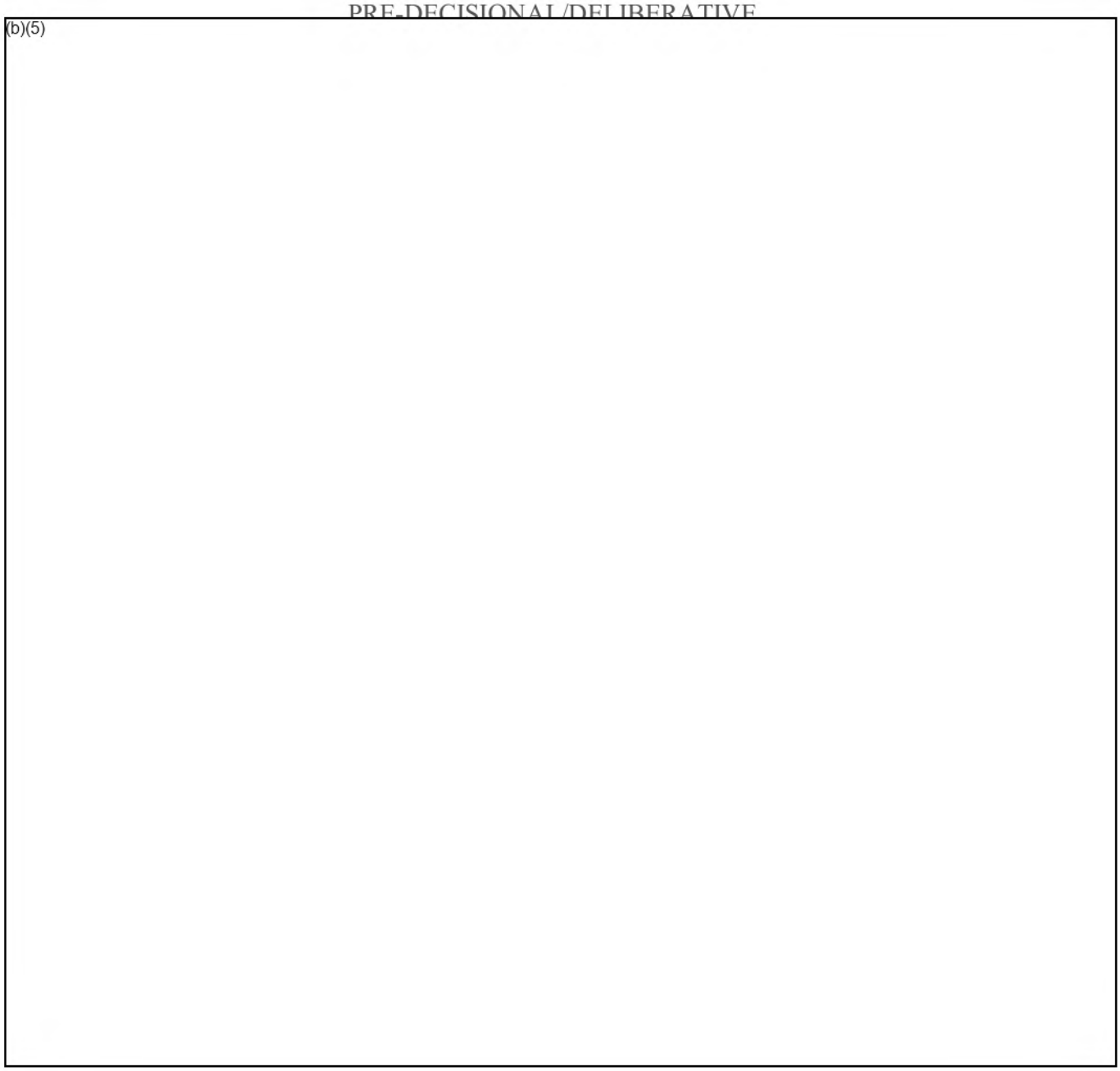
MEMORANDUM FOR THE DIRECTOR

FROM: Bradford Willke
Acting Assistant Dir (b)(6)

SUBJECT: (b)(5)

(b)(5)

(b)(5)



(b)(5)

11/13/2020

(b)(6)

Approve/date Disapprove/date_____

Modify/date _____ Needs discussion/date_____

Attachments:

(b)(5)

U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Office of the Director
Washington, DC 20528

November 13, 2020

DECISION

MEMORANDUM FOR THE ACTING SECRETARY

FROM: Christopher C. Krebs (b)(6)
Director

SUBJECT: (b)(5)

(b)(5)

(b)(5)

(b)(6); (b)(5)

(b)(5)

(b)(5)

Approve/date_____ Disapprove/date_____

Modify/date _____ Needs discussion/date_____

Attachment(s):

(b)(5)

U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
National Risk Management Center
Washington, DC 20528

October 14, 2020

DECISION

MEMORANDUM FOR THE DIRECTOR

FROM: Bob Kolasky
Assistant Director (b)(6)

SUBJECT: (b)(5)

(b)(6); (b)(5)

(b)(5)

Approve/date (b)(6) **11/05/2020**

Disapprove/date_____

Modify/date _____

Needs discussion/date_____

Attachment(s):

1. (b)(5)

U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Infrastructure Security Division
Washington, DC 20528

October 16, 2020

DECISION

MEMORANDUM FOR THE DIRECTOR (b)(6)

FROM: Steve Harris
Assistant Director (A)

SUBJECT: (b)(5)

(b)(6); (b)(5)

(b)(5)

(b)(6)

11/05/2020

Approve/dat

Disapprove/date_____

Modify/date _____ Needs discussion/date_____

Attachments:

(b)(5)

U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Office of the Director
Washington, DC 20528

November 16, 2020

Mr. (b)(6)
Member
The President's National Infrastructure Advisory Council
(b)(6)

Dea (b)(6)

I would like to express my gratitude for your service on the President's National Infrastructure Advisory Council (NIAC). The Department has greatly benefited from your leadership, ideas, and experience.

I would like to specifically thank you for your service co-chairing the 2017 *Securing Cyber Assets* study and scoping effort, resulting in specific recommendations on how federal authorities and capabilities can be best applied to secure critical infrastructure assets. I would also like to recognize your current support as a member of the Workforce and Talent Management Study Working Group, providing your expertise on how we can help prevent workforce challenges from impacting critical infrastructure. Your contributions to those efforts helped identify actionable solutions to ensure the security and resilience of our infrastructure and provided tremendous value to the nation. Thank you for your time and service.

Sincerely,

(b)(6)

Christopher C. Krebs
Director

U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Office of the Chief Information Officer
Washington, DC 20528

November 2, 2020

DECISION

MEMORANDUM FOR THE DEPUTY DIRECTOR

FROM: (b)(6)
Chief Information Officer (Acting) (b)(6)

SUBJECT: (b)(6); (b)(5)

(b)(6); (b)(5); (b)(7)(E)

(b)(6); (b)(5); (b)(7)(E)

(b)(6); (b)(5); (b)(7)(E)

Approve/date (b)(6) 6NOV2020 Disapprove/date_____

Modify/date _____ Needs discussion/date_____

U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Office of the Director
Washington, DC 20528

November 10, 2020

MEMORANDUM FOR THE ACTING CHIEF OF STRATEGY, POLICY, AND PLANS; ACTING DEPUTY ASSISTANT DIRECTOR FOR CYBERSECURITY; CHIEF HUMAN CAPITAL OFFICER

FROM: Matthew Travis (b)(6)
Deputy Director

SUBJECT: **Action: Cybersecurity Detail Assignment Commitment fo** (b)(6) (b)(6)

Purpose: This memorandum memorializes the commitment and directs the eventual action to honor an intra-agency detail assignment within the Cybersecurity and Infrastructure Security Agency (CISA) for (b)(6) from the Office of Strategy, Policy, and Plans (SPP) to the Cybersecurity Division (CSD) at the earliest opportunity practicable.

Context: In the summer of 2020, (b)(6) applied for, and was accepted to, a cybersecurity detail assignment within the Cyber Threat Information Sharing (CTIS) team of CSD. Due to manpower shortages and an uncertain impending workload within (b)(6) branch, SPP leadership was unable to approve the detail assignment at the time her application was accepted.

CISA leadership has determined that it is in the long-term interest of the Agency to train and develop its workforce, especially as it pertains to technical cybersecurity experience for women. This detail for (b)(6) s in furtherance of said Agency objective and therefore it is important that it be fulfilled soonest.

Directed Actions: The following CISA elements will take the appropriate action detailed below, at the earliest opportunity possible, in support of (b)(6) detail to CSD/CTIS:

1. SPP will hire additional personnel or reallocate its project portfolio to allow (b)(6) to embark on the CSD detail no later than March 31, 2021.
2. CSD will ensure said detail assignment remains open, or an additional detail position be created, to support (b)(6) assignment to CTIS.
3. The Office of the Chief Human Capital Officer will administer the requisite processes and documentation to support (b)(6) detail.

U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Office of the Director
Washington, DC 20528

November 10, 2020

The Honorable Catherine Cortez Masto
United States Senate
Washington, DC 20510

Dear Senator Cortez Masto

Thank you for your letter dated October 2, 2020, to the Department of Homeland Security (DHS) regarding cybersecurity and our Nation's K-12 schools. Acting Secretary Wolf asked that I respond on his behalf.

We appreciate your interest in the Cybersecurity and Infrastructure Security Agency's (CISA) efforts to build the national capacity to defend against cyber-attacks. Cyber threats remain one of the most significant strategic risks for our Nation, threatening our security, economic prosperity, and public safety. During the COVID-19 pandemic, businesses, organizations, and governments have become increasingly vulnerable to ransomware attacks. In the case of school districts, cyber incidents can severely impact student access to education and instruction, as well as potentially expose sensitive information.

CISA has been working to ensure that state and local governments and school districts have access to resources to strengthen their cybersecurity posture. Recently, we released the CISA Cyber Essentials guide to help leaders understand how to implement organizational cybersecurity practices and recently issued, with the Multi-State Information Sharing and Analysis Center (MS-ISAC), a Ransomware Guide to enhance network defense to a ransomware attack. This guide includes best practices to prevent, respond to, and quickly recover from ransomware attacks. We have provided your staff with a copy of the Guide.

To fully address your letter, we would like to brief you and your staff. This briefing would include an in-depth discussion about the services and tools available to support state, local, tribal, and territorial government entities, including school systems, as they strengthen their cyber defenses.

Thank you again for your letter. The co-signer of your letter will receive a separate, identical response. Should you wish to discuss this further, please do not hesitate to contact me.

Sincerely,

(b)(6)

Christopher C. Krebs
Director

U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Office of the Director
Washington, DC 20528

November 10, 2020

The Honorable Jacky Rosen
United States Senate
Washington, DC 20510

Dear Senator Rosen:

Thank you for your letter dated October 2, 2020, to the Department of Homeland Security (DHS) regarding cybersecurity and our Nation's K-12 schools. Acting Secretary Wolf asked that I respond on his behalf.

We appreciate your interest in the Cybersecurity and Infrastructure Security Agency's (CISA) efforts to build the national capacity to defend against cyber-attacks. Cyber threats remain one of the most significant strategic risks for our Nation, threatening our security, economic prosperity, and public safety. During the COVID-19 pandemic, businesses, organizations, and governments have become increasingly vulnerable to ransomware attacks. In the case of school districts, cyber incidents can severely impact student access to education and instruction, as well as potentially expose sensitive information.

CISA has been working to ensure that state and local governments and school districts have access to resources to strengthen their cybersecurity posture. Recently, we released the CISA Cyber Essentials guide to help leaders understand how to implement organizational cybersecurity practices and recently issued, with the Multi-State Information Sharing and Analysis Center (MS-ISAC), a Ransomware Guide to enhance network defense to a ransomware attack. This guide includes best practices to prevent, respond to, and quickly recover from ransomware attacks. We have provided your staff with a copy of the Guide.

To fully address your letter, we would like to brief you and your staff. This briefing would include an in-depth discussion about the services and tools available to support state, local, tribal, and territorial government entities, including school systems, as they strengthen their cyber defenses.

Thank you again for your letter. The co-signer of your letter will receive a separate, identical response. Should you wish to discuss this further, please do not hesitate to contact me.

Sincerely,

(b)(6)

Christopher C. Krebs
Director

U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Office of the Director
Washington, DC 20528

November 17, 2020

The Honorable Marco Rubio
United States Senate
Washington, DC 20510

Dear Senator Rubio:

Thank you for your letter dated September 2, 2020, regarding cybersecurity and our Nation's K-12 school systems. We appreciate your interest and commitment to the Cybersecurity and Infrastructure Security Agency's (CISA) efforts to build the national capacity to defend against cyber attacks.

Cyber threats remain one of the most significant strategic risks for our Nation, threatening our security, economic prosperity, and public safety. During the COVID-19 pandemic, businesses, organizations, and governments throughout our communities have become increasingly vulnerable to ransomware attacks. In the case of school districts, cyber incidents can severely impact student access to education and instruction, as well as potentially expose sensitive information.

CISA has been working to ensure that state and local governments and agencies – including school districts - have access to resources that can help to strengthen their cyber posture. Over the summer, we released the CISA Cyber Essentials Toolkit to help leaders understand where and how to start implementing organizational cybersecurity practices and recently issued, with the Multi-State Information Sharing and Analysis Center (MS-ISAC), a Ransomware Guide to enhance network defense and reduce exposure to a ransomware attack. This guide is a one-stop resource with best practices to not only prevent ransomware attacks, but to also respond to and recover quickly. We have provided your staff with a copy of the Ransomware Guide.

We have been working with your staff on this issue and provided a briefing on September 22, 2020, highlighting services and tools that the Agency has available to support state, local, tribal, and territorial (SLTT) government entities, including school systems, to improve their cyber posture. We stand ready to provide additional briefings at your convenience. We will continue to update you on our efforts to support SLTT governments – including school districts – and look forward to working with you to defend today and secure tomorrow.

Thank you again for your letter. Should you wish to discuss this further, please do not hesitate to contact me.

Sincerely,

(b)(6)

Christopher C. Krebs
Director

U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Stakeholder Engagement Division
Washington, DC 20528

October 20, 2020

DECISION

MEMORANDUM FOR THE DIRECTOR

THROUGH: Bradford Willke
Acting Assistant Director, Stakeholder Engagement Division
(b)(6)

FROM: Susan May
Branch Chief for International Affairs
(b)(6)

SUBJECT: (b)(5)

(b)(6); (b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(6) 11/6/20

Approve/da_____ Disapprove/date_____

Modify/date_____ Needs discussion/date_____

Attachments:

(b)(5)

U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Office of the Director
Washington, DC 20528

November 16, 2020

DECISION

MEMORANDUM FOR THE ACTING SECRETARY

FROM: Christopher C. Krebs (b)(6)
Director

SUBJECT: (b)(5)

(b)(5)

(b)(5)

Approve/date_____ Disapprove/date_____

Modify/date _____ Needs discussion/date_____

Attachment(s):

(b)(6)

U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Emergency Communications Division
Washington, DC 20528

November 3, 2020

DECISION

MEMORANDUM FOR THE DIRECTOR

FROM: Billy Bob Brown Jr. (b)(6)
Assistant Director

SUBJECT: (b)(5)

(b)(6)

(b)(5)

(b)(6) 11/17/20

Approve/da

Disapprove/date_____

Modify/date _____

Needs discussion/date_____

Attachments:

(b)(5)

U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Infrastructure Security Division
Washington, DC 20528

October 26, 2020

DECISION

MEMORANDUM FOR THE DIRECTOR (b)(6)

FROM: Steven Harris
Acting Assitant Director for Infrastructure Security

SUBJECT: (b)(5)

(b)(6); (b)(5)

(b)(5)

(b)(6) 11/17/20

Approve/d

Disapprove/date_____

Modify/date _____ Needs discussion/date_____

Attachment:

(b)(5)

U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Stakeholder Engagement Division
Washington, DC 20528

October 20, 2020

DECISION

MEMORANDUM FOR THE DIRECTOR

FROM: Bradford Willke (b)(6)
Assistant Director (Acting) for Stakeholder Engagement

SUBJECT: (b)(5)

(b)(6); (b)(5)

(b)(5)

11/16/20

(b)(6)

Approve/date

Disapprove/date_____

Modify/date _____

Needs discussion/date_____

Attachment(s):

(b)(5)

U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Stakeholder Engagement Division
Washington, DC 20528

October 13, 2020

DECISION

MEMORANDUM FOR THE DIRECTOR

FROM: Bradford Willke
Acting Assistant Dire (b)(6)

SUBJECT: (b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(6) 1/13/2020

Approve/date

Disapprove/date_____

Modify/date _____ Needs discussion/date_____

Attachments:

(b)(5)

U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Office of the Director
Washington, DC 20528

November 6, 2020

Executive Committee (Samoa, Tonga, and Vanuatu)
Pacific Cyber Security Operational Network (PaCSON)
R.G. Casey Building
John McEwen Crescent
Barton ACT 0221 Australia

Dear Executive Committee Members,

The Cybersecurity and Infrastructure Security Agency (CISA) welcomes the opportunity to join PaCSON. As the United States' risk advisor, CISA works with partners to defend against today's threats and collaborate to build more secure and resilient for the future. CISA builds the national capacity to defend against cyber-attacks and also works with the U.S. federal government; state, local, tribal and territorial (SLTT) governments; private industry; academia; NGOs and non-profits; international partners; and general public stakeholders to provide cybersecurity tools, incident response services, and assessment capabilities.

CISA's Stakeholder Engagement Division helps the agency craft strategic engagements that forge partnerships, facilitate dialogue, convene stakeholders, and promote awareness to advance CISA's mission. In line with these goals, I am pleased to endorse CISA's application to officially join PaCSON as a Partner. CISA is eager to foster engagement with the Indo-Pacific region and hopes to work through PaCSON to promote information sharing and expert insight into threat activity with PaCSON member countries. Through this exciting new engagement and increased information sharing, we hope to build strong and enduring relationships with PaCSON member countries.

If our application is approved, CISA looks forward to collaborating with PaCSON and identifying ways that CISA can contribute meaningfully to cybersecurity collaboration in the Indo-Pacific region.

Thank you for considering our application. Should you have any questions or need to reach out to CISA about our application, please contact CISA International Affairs Branch Chief (b)(6) (b)(6) at CISAInternationalAffairs@hq.dhs.gov or (b)(6)

Sincerely,

(b)(6)

Christopher Krebs
Director

U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Office of the Director
Washington, DC 20528

November 16, 2020

Mr. Robert Carr
Member
The President's National Infrastructure Advisory Council
82 Library Place
Princeton, New Jersey 08540

Dear Mr. Carr,

I would like to express my gratitude for your service on the President's National Infrastructure Advisory Council (NIAC). The Department has greatly benefited from your leadership, ideas, and experience.

I would like to specifically thank you for your service co-chairing the 2017 *Securing Cyber Assets* study and scoping effort, resulting in specific recommendations on how federal authorities and capabilities can be best applied to secure critical infrastructure assets. I would also like to recognize your current support as a member of the Workforce and Talent Management Study Working Group, providing your expertise on how we can help prevent workforce challenges from impacting critical infrastructure. Your contributions to those efforts helped identify actionable solutions to ensure the security and resilience of our infrastructure and provided tremendous value to the nation. Thank you for your time and service.

Sincerely,

(b)(6)

Christopher C. Krebs
Director