

FW: 2022-12-22 NCD and PDNCD Briefing Book

From: "Chang, Caroline EOP/NCD" <(b) (6)>
To: "Knake, Robert K. EOP/NCD" <(b) (6)>, "DeRusha, Chris J. EOP/OMB" <(b) (6)>, "Higgins, Neal L. EOP/NCD" <(b) (6)>, "Stewart Gloster, Camille A. EOP/NCD" <(b) (6)>
Cc: DL ExecSec <(b) (6)>, "Hochman, Michael C. EOP/NCD" <(b) (6)>, "Klein, Julie G. EOP/NCD" <(b) (6)>, "Fontanez, Jose A. EOP/NCD" <(b) (6)>, "Haas, Benjamin E. EOP/NCD" <(b) (6)>, "Reynolds, Gevin B. EOP/NCD" <(b) (6)>, "Ring, Haley A. EOP/NCD" <haley.a.ring@ncd.eop.gov>
Date: Wed, 21 Dec 2022 11:12:00 -0500
Attachments: 1. Mtg. Agenda Leg Affairs Bi-weekly.pdf (569.81 kB); 2. Decision Memo_Intl Engagement Strategy (Clean).pdf (345.35 kB); 3. Open Source Software Security Initiative.pdf (805.15 kB); 4. Briefing Memo - HATWH Event Concept.pdf (112.44 kB); 5. Briefing Memo - Africa Leaders Summit Readout.pdf (94.93 kB); 6. Space Executive Forum - Participant List and Agenda.pdf (268.56 kB); NCD - Daily Schedule.docx (91.45 kB); PDNCD - Daily Schedule.docx (91.09 kB)

Dear Deputies, please see attached a soft copy of NCD and PDNCD's briefing book.

Best,
Caroline

Caroline Chang
Senior Advisor to NCD and ExecSec
Office of the National Cyber Director
Executive Office of the President
(b) (6)

From: Chang, Caroline EOP/NCD
Sent: Wednesday, December 21, 2022 11:11 AM
To: Inglis, Chris C. EOP/NCD <(b) (6)>; Walden, Kemba E. EOP/NCD <(b) (6)>
Cc: DL ExecSec <(b) (6)>; Hochman, Michael C. EOP/NCD <(b) (6)>
Subject: 2022-12-22 NCD and PDNCD Briefing Book

Dear Chris and Kemba,

Please see attached your briefing book for tomorrow and the weekend. We are including a few of the papers we transmitted to you yesterday so you have all your holiday reading in one place. Please let us know if you have any questions.

1. Bi weekly Leg Affairs Sync Agenda + Read Ahead Materials
2. Decision Memo on International Strategy
3. Briefing Memo on Open Source Software Security Initiative

4. Briefing Memo on Hackers at the White House Event
5. Briefing Memo on Africa Leaders Summit Readout
6. Draft participant list and agenda for the Space Executive Forum
 - Please see the accompanying cover paragraph in the email enclosed

Best,
Caroline

Caroline Chang

Senior Advisor to NCD and ExecSec
Office of the National Cyber Director
Executive Office of the President

(b) (6)

UNCLASSIFIED//FOR OFFICIAL USE ONLY

**MEMORANDUM FOR THE DEPUTY NATIONAL CYBER DIRECTOR
FOR TECHNOLOGY & ECOSYSTEM SECURITY**

FROM: Anjana Rajan
Assistant National Cyber Director
Technology Security

Seeyew Mo
Assistant National Cyber Director
Cyber Workforce

Eric Mill
Senior Advisor
Office of the Federal Chief Information Officer

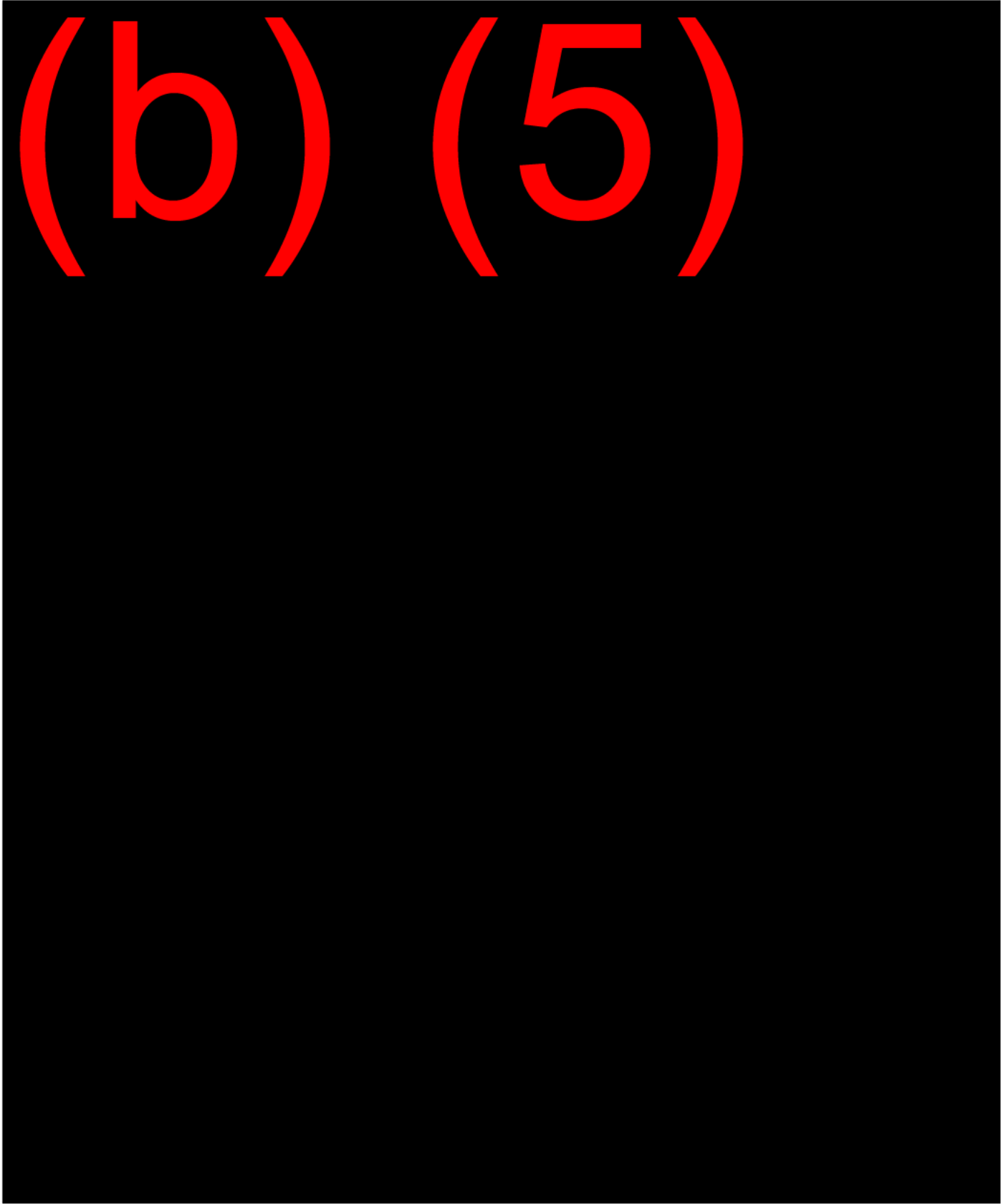
Conrad Stosz
Policy Advisor
Office of the Federal Chief Information Officer

DATE: December 7, 2022

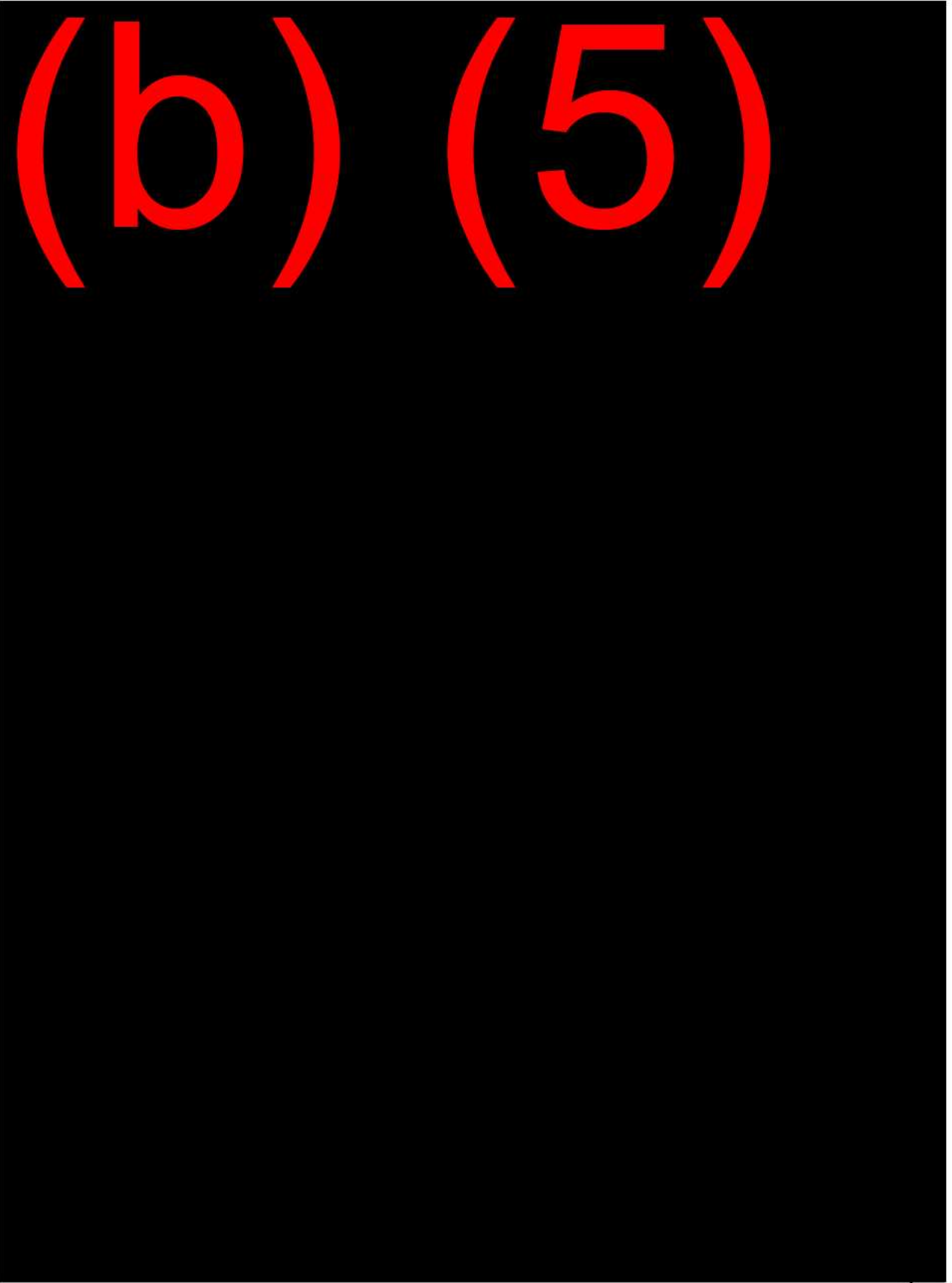
SUBJECT: Open-Source Software Security Initiative (OS3I):
2022 Strategic Recommendations (Phase I) & 2023 Implementation Initiatives (Phase II)

(b) (5)

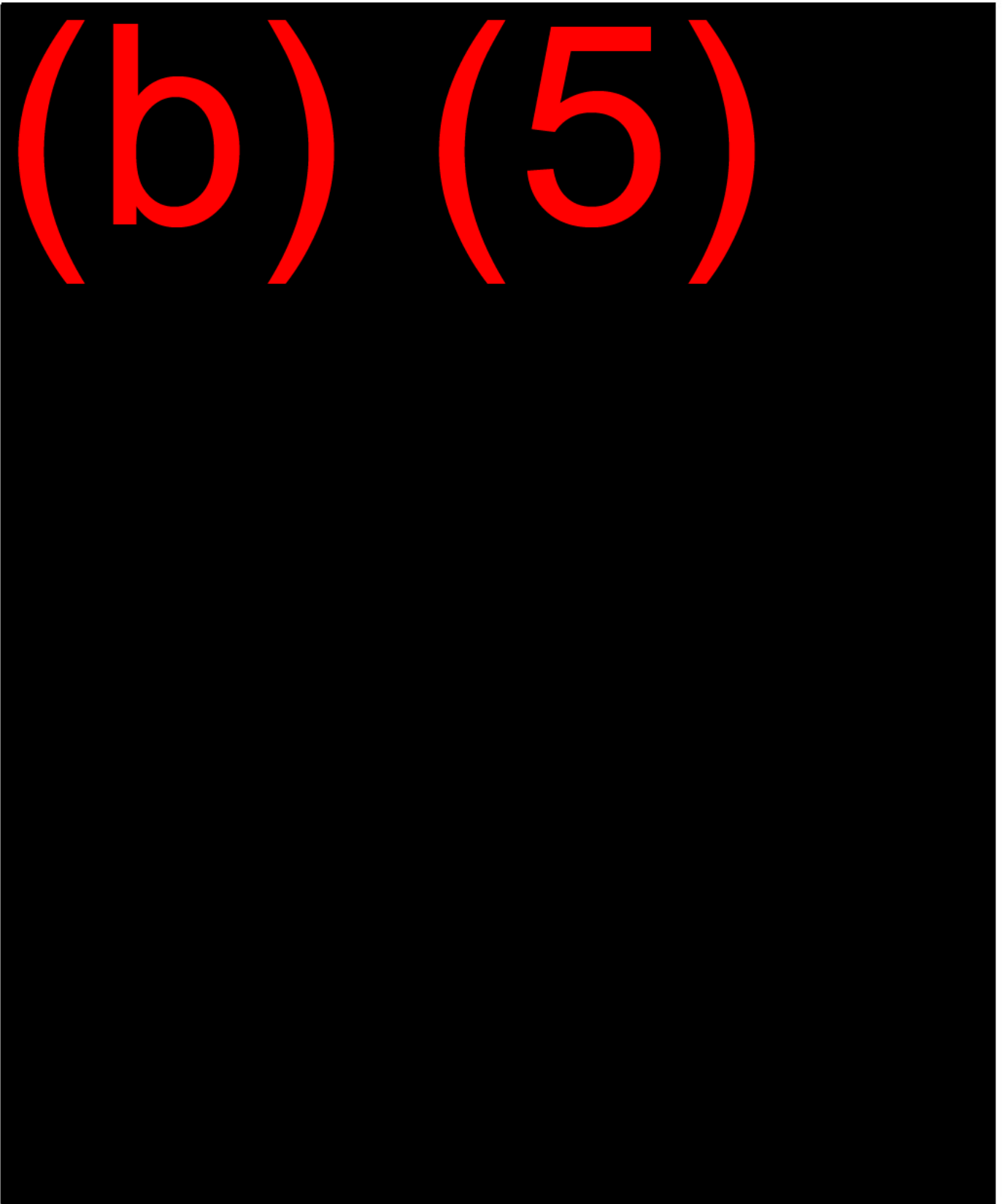
(b) (5)



(b) (5)



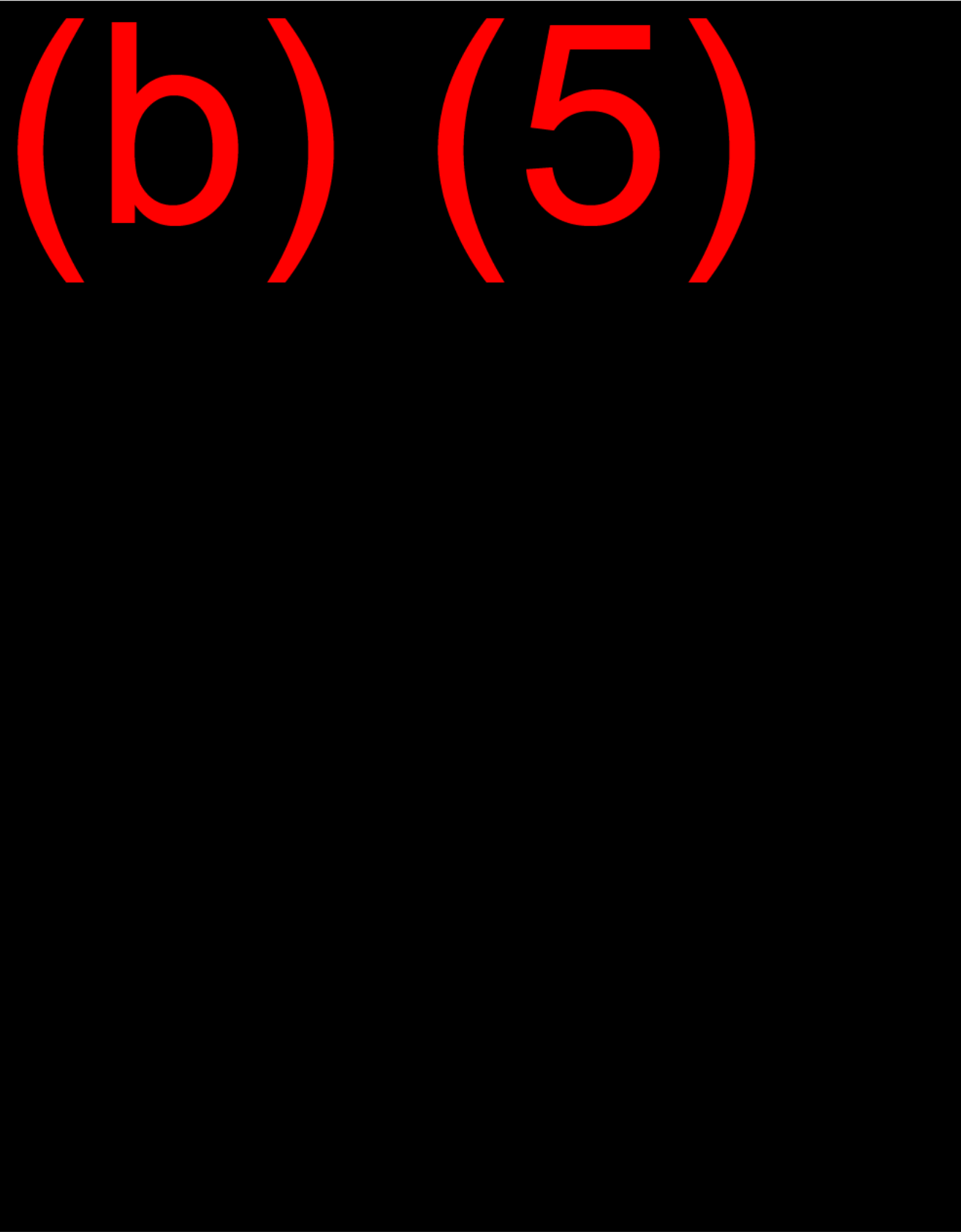
(b) (5)



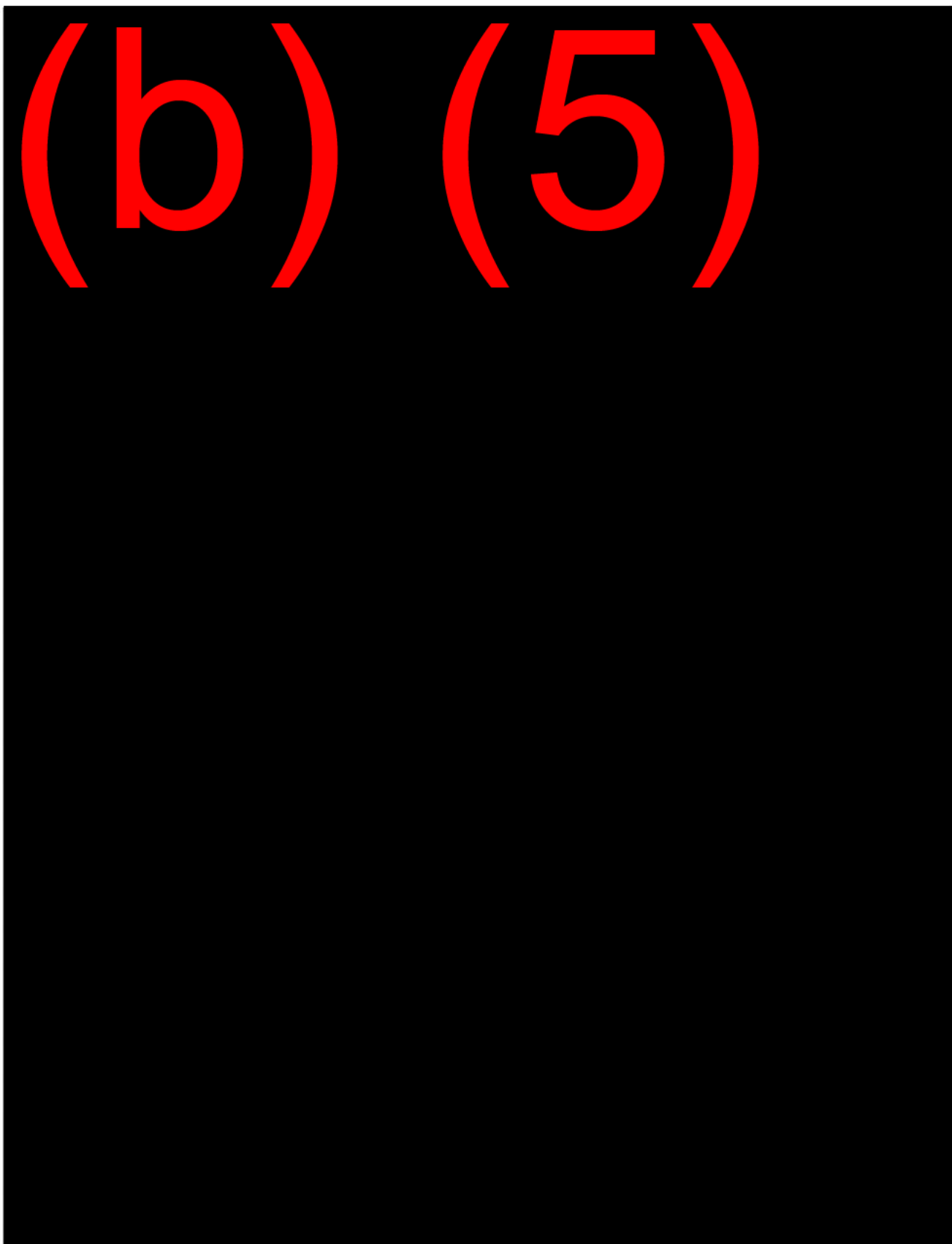
(b) (5)

(b) (6)

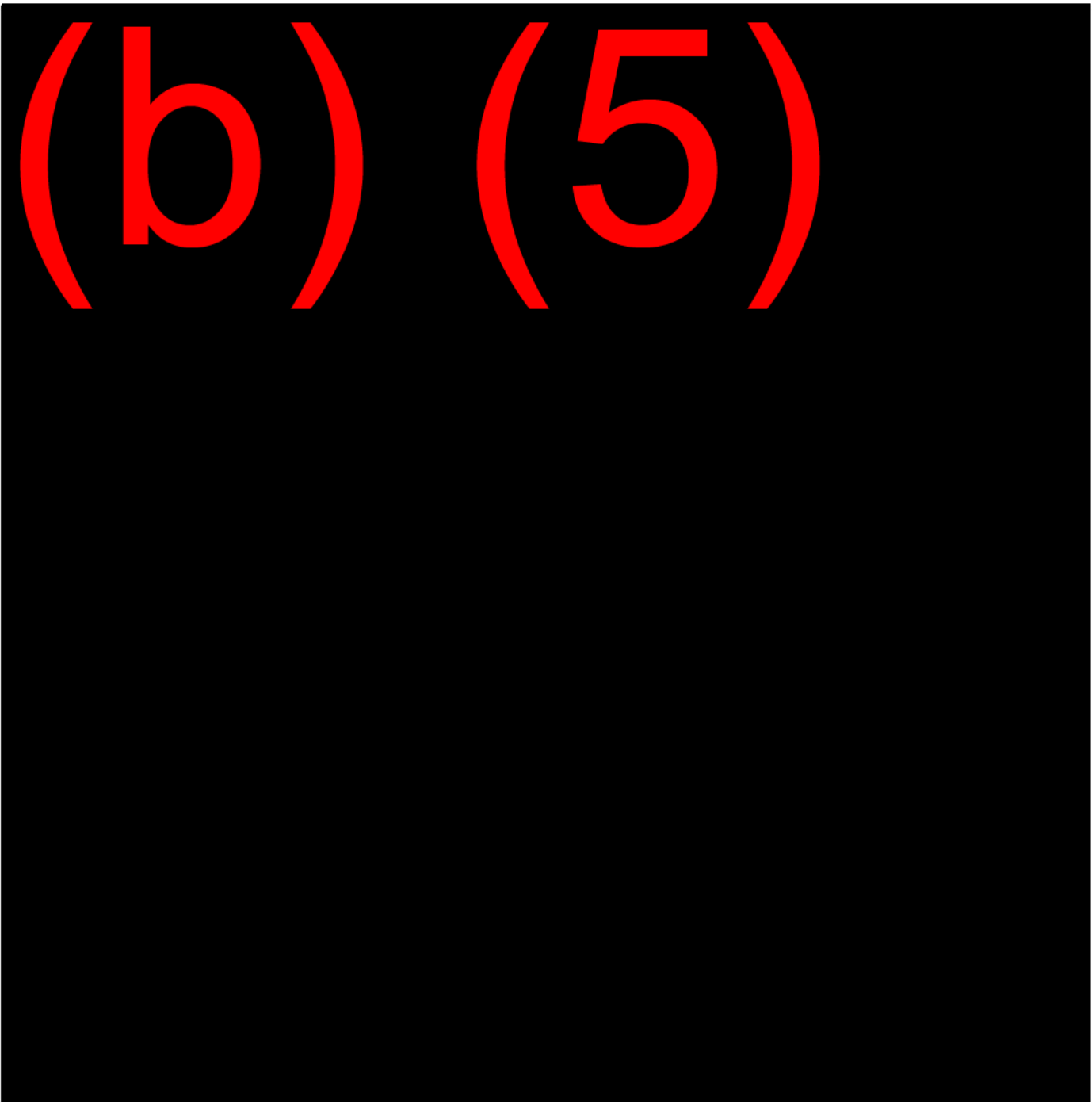
(b) (5)



(b) (5)



(b) (5)



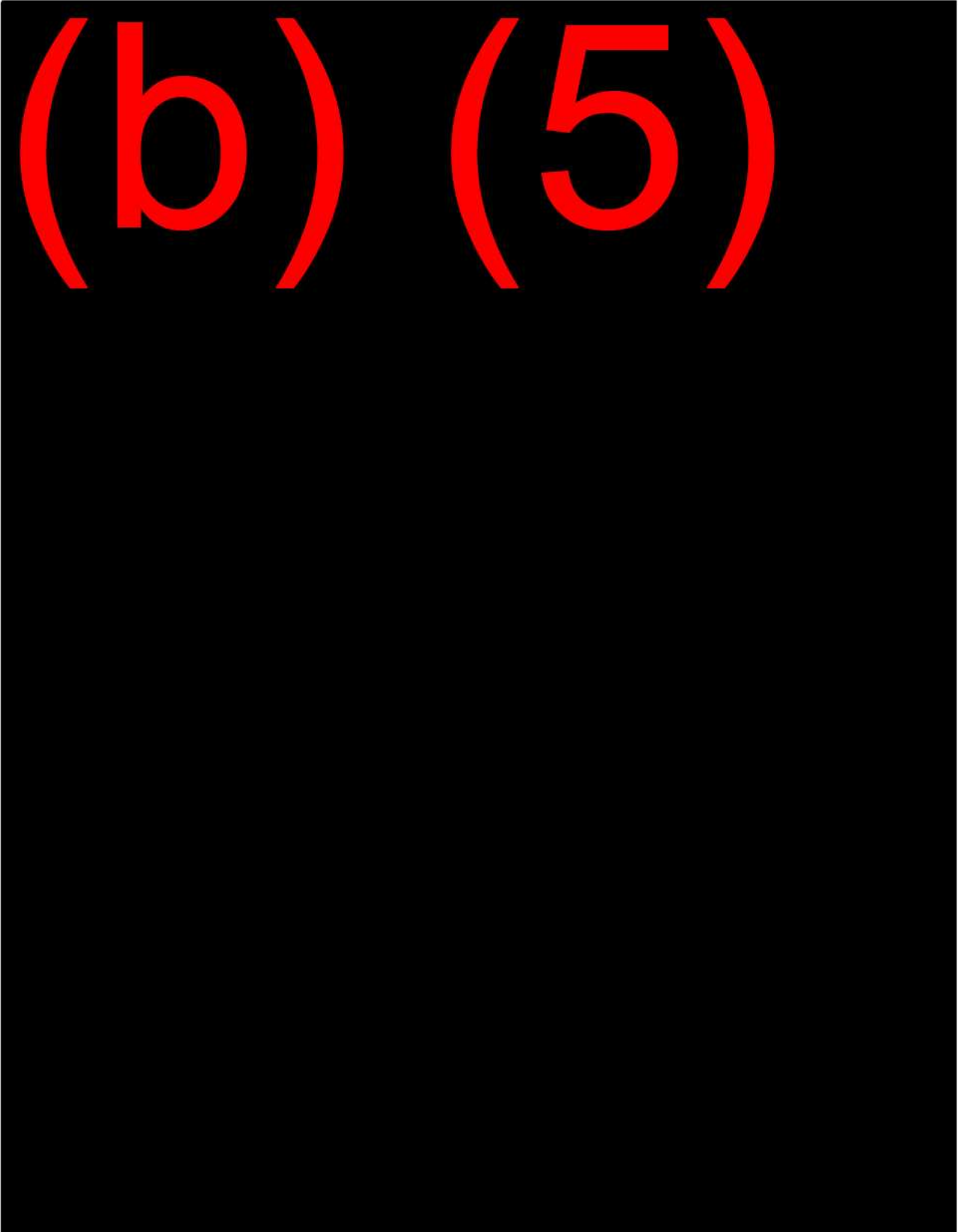
Approval and Coordination Decision

Attachment B: Open-Source Software Security Initiative – Executive Summary

Approve: _____	Approve as Amended: _____
Reject: _____	Discuss: _____

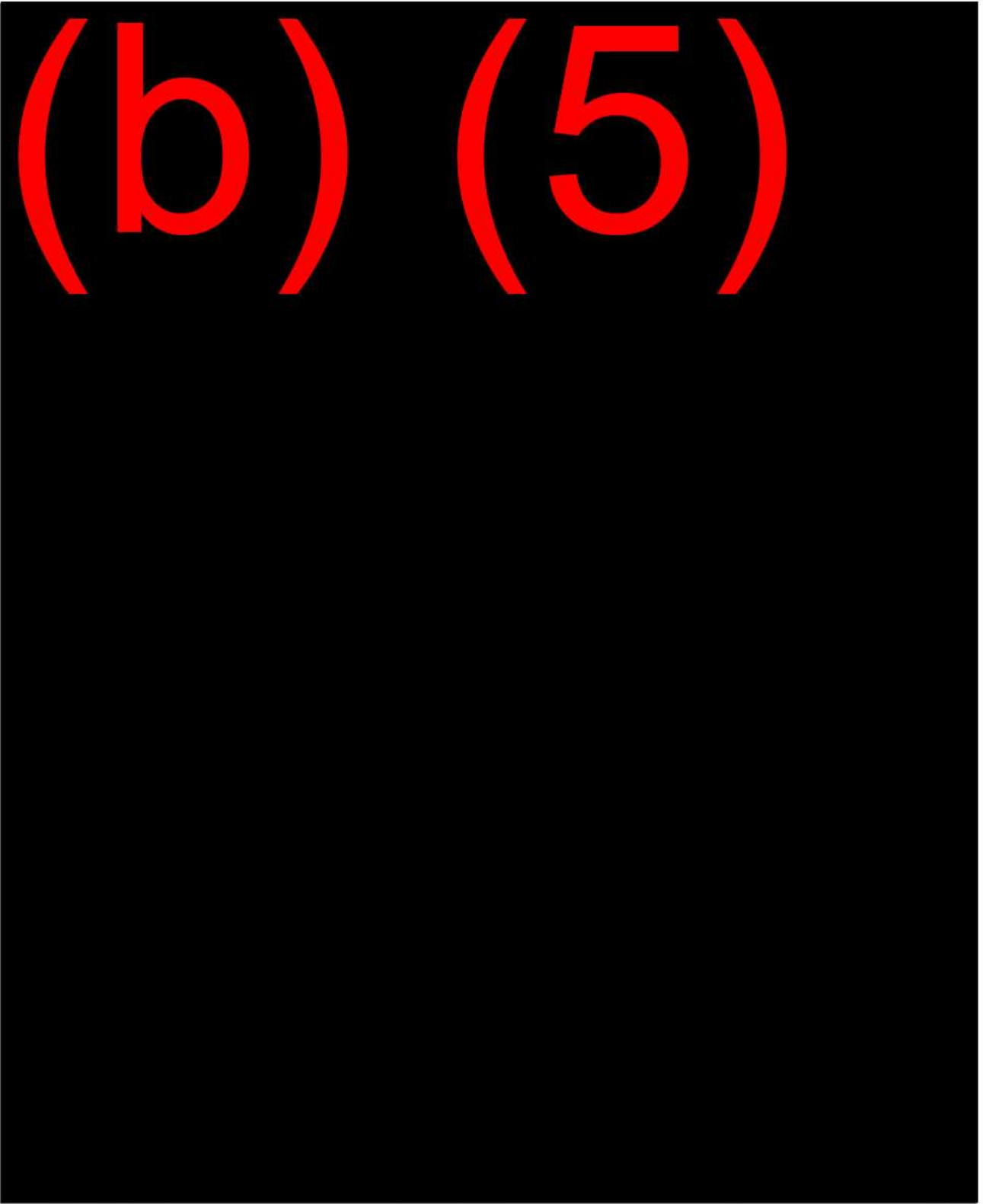
CAMILLE STEWART Digitally signed by CAMILLE STEWART Date: 2022.12.19 10:36:17 -05'00'	_____ DATE
CAMILLE STEWART GLOSTER Deputy National Cyber Director, TES Office of the National Cyber Director Executive Office of the President	

(b) (5)

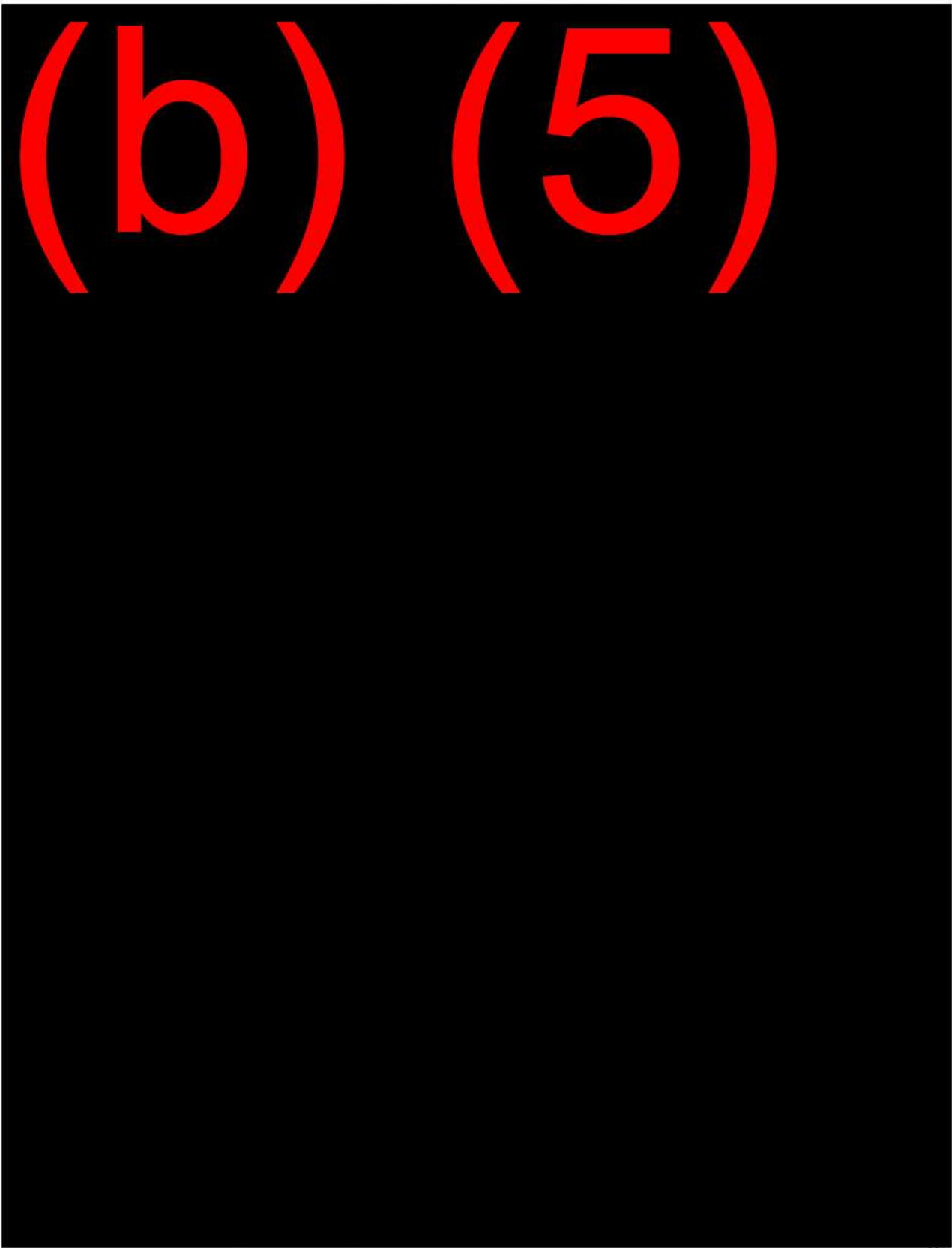


BACKGROUND

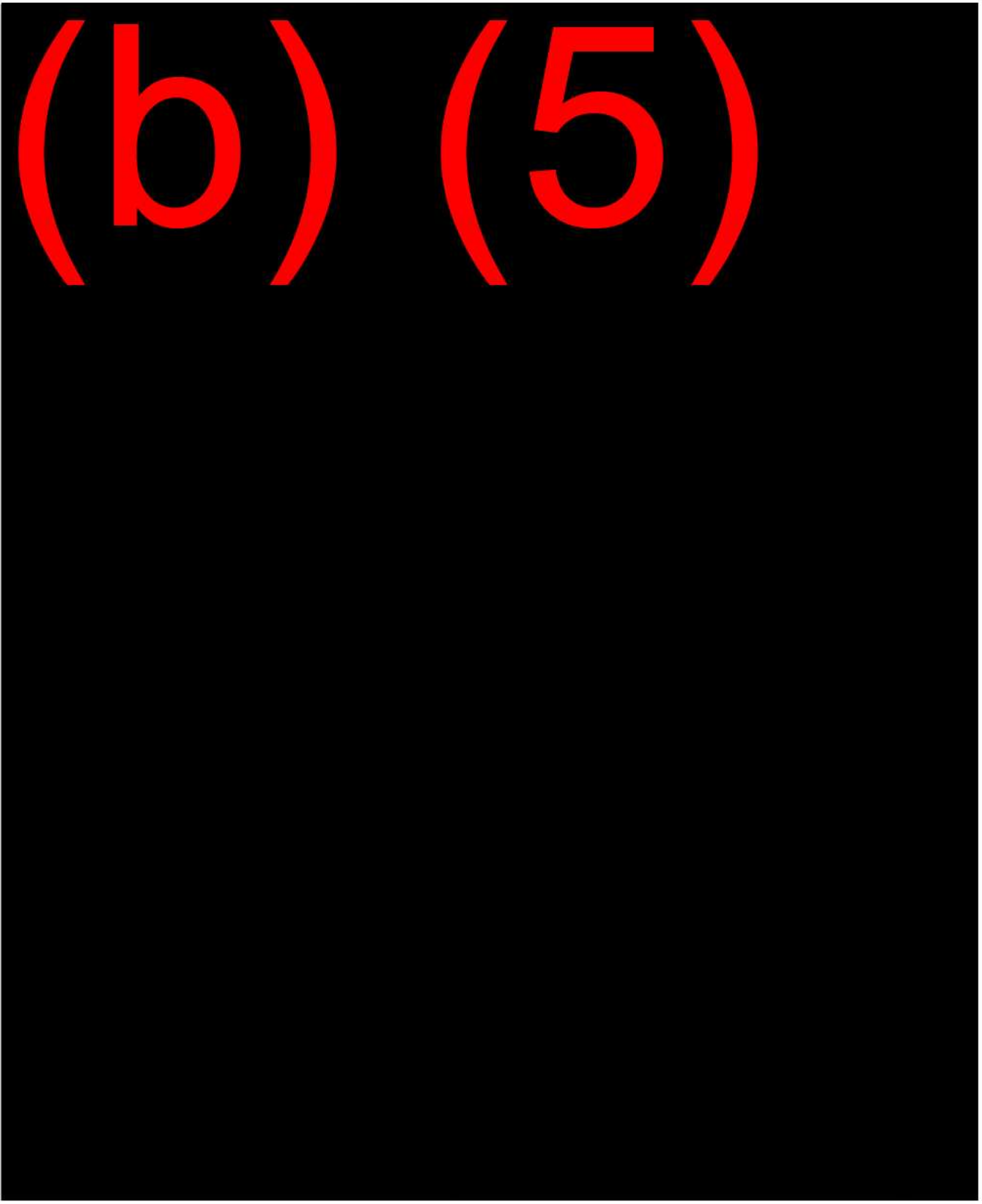
(b) (5)



(b) (5)

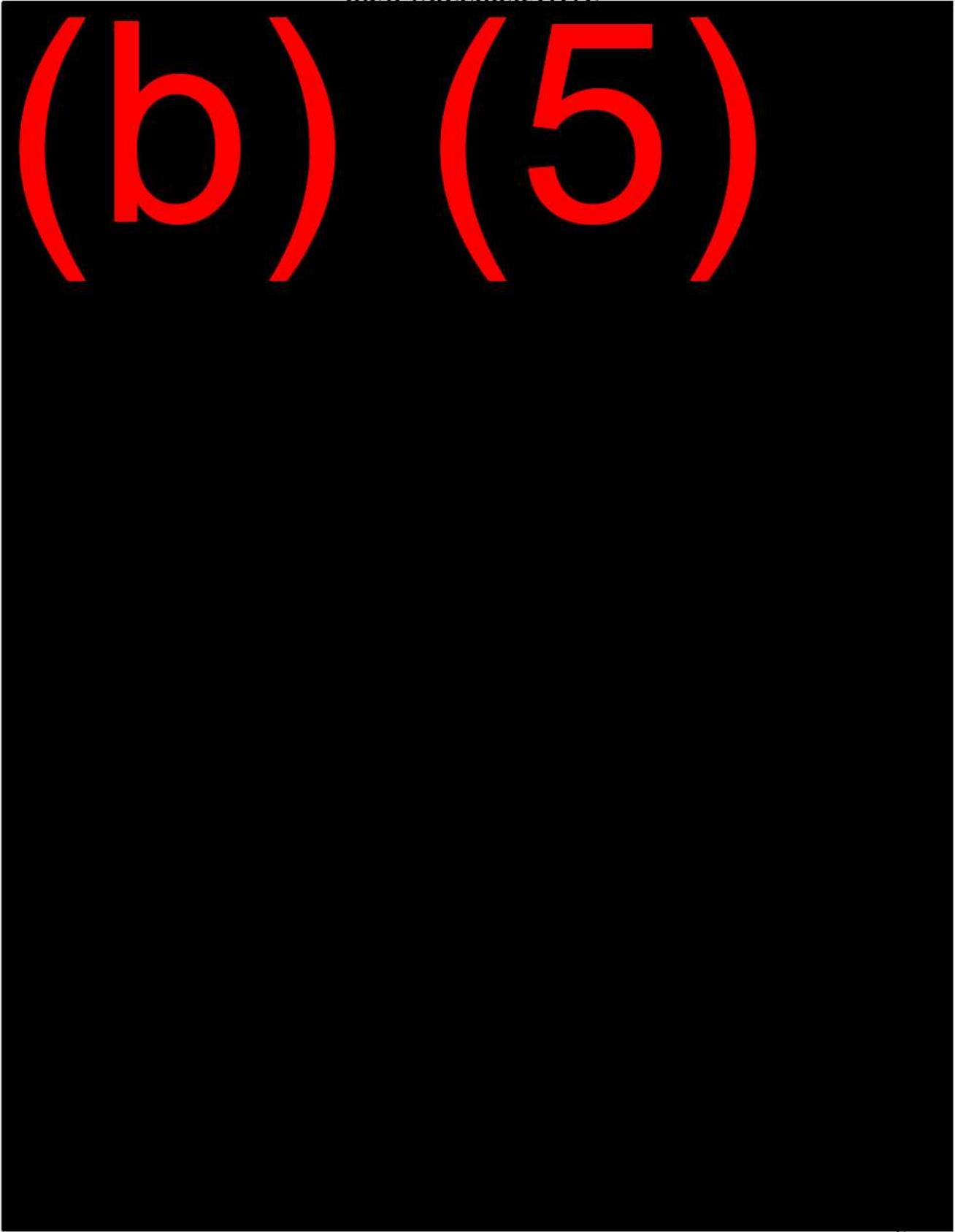


(b) (5)

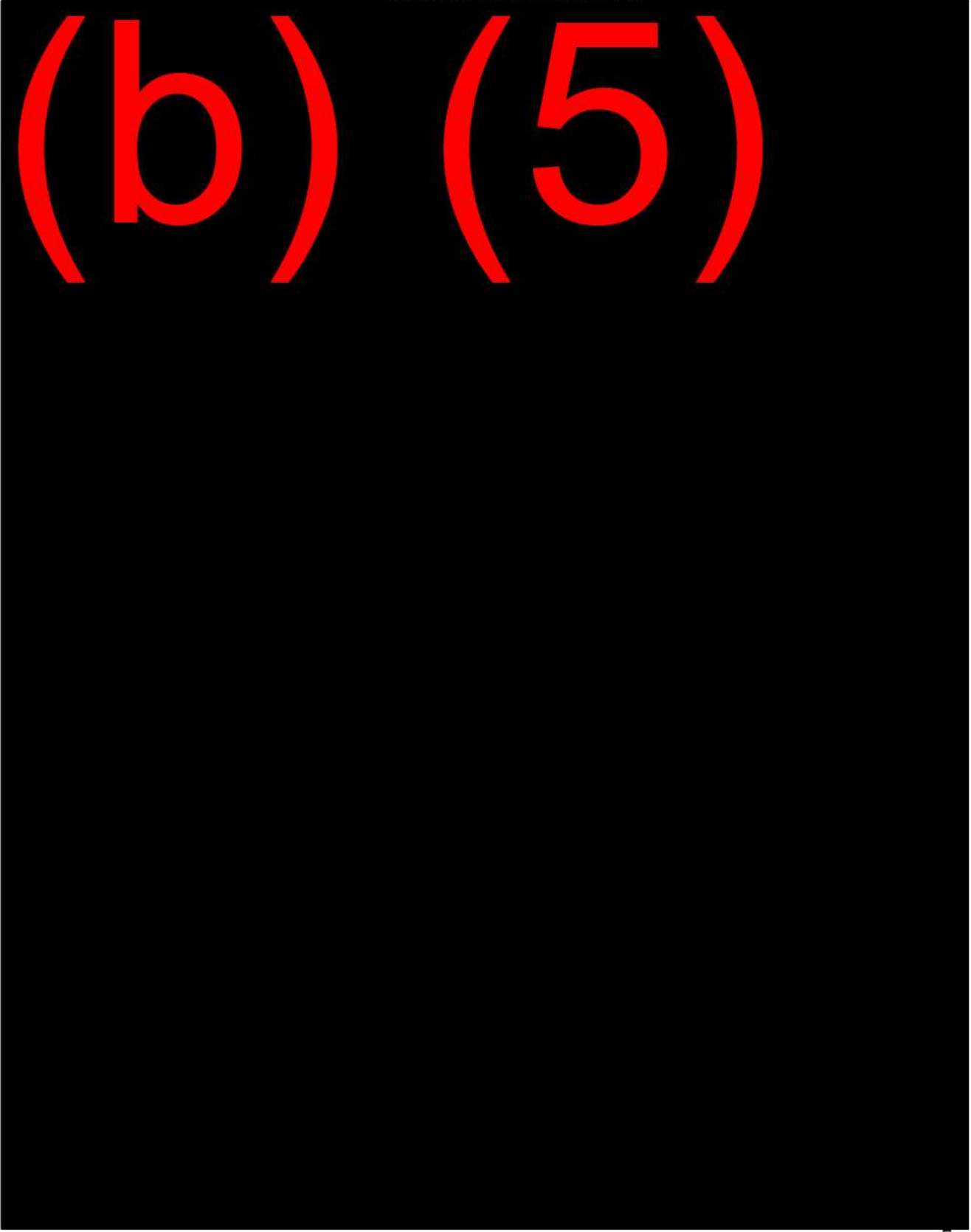


(b) (5)

(b) (5)



(b) (5)



(b) (5)



Open Source Software Security Initiative (OS3I)

(b) (5)

(b) (5)

Chang, Caroline EOP/NCD

From: Rajan, Anjana EOP/NCD
Sent: Tuesday, December 20, 2022 4:15 PM
To: Chang, Caroline EOP/NCD
Cc: Leiserson, Nick J. EOP/NCD; Williams, Lauryn D. EOP/NCD; Simms, Tanya L. EOP/NCD; Krejsa, Harry H. EOP/NCD; Scott, Brian C. EOP/NCD; Corell, Joyce E. EOP/NCD; Berlin, Jen S. EOP/NCD
Subject: [for NCD/PDNCD] Space Forum - Proposed Attendee List and Agenda
Attachments: Space Executive Forum - Participant List & Agenda.docx

Hi Caroline,

Linked and attached is our due out for Chris and Kemba on the [proposed attendees and agenda for the Space Forum](#). I've included a paragraph to include with this deliverable. Please let us know if you need anything from us on this!

Warmly,
Anjana

--

Dear Chris and Kemba,

Pursuant to our meeting last Tuesday, we have put together a draft attendee list and draft agenda. We look forward to hearing your comments. Our next step will be to begin socializing this with our interagency partners. We look forward to briefing you in the new year about our SPD-5 implementation plan and our progress on the Space Forum.

Thanks,
Space Team

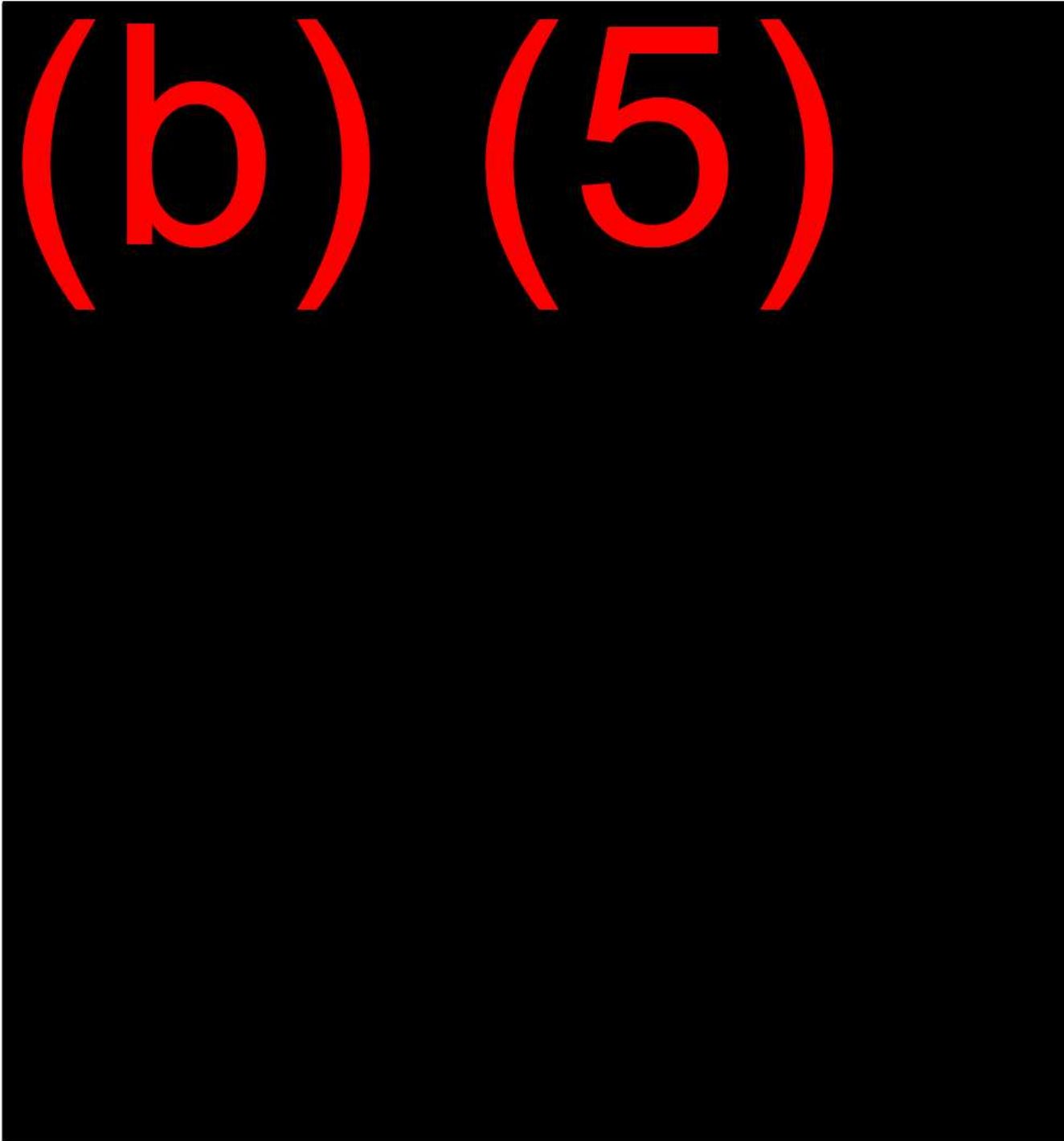
--

Anjana Rajan
Assistant National Cyber Director, Technology Security
Office of the National Cyber Director

(b) (6) | (b) (6)

Space Executive Forum
Proposed Participant List & Agenda

(b) (5)



Draft Agenda

- Intelligence Threat Briefing (1'50")
- Transition (0'10")
- Opening Remarks – USG (0'20")
- Discussion – all (1'05")
 - SPD-5 Implementation Plan Pillars
- Closing remarks/summary – NCD/VPOTUS (0'05")
- [Press gaggle – VPOTUS/NCD (0'15")]
- [Reception (1'15")]

Total Time: 3'30" (sans press gaggle and reception.) Can be hosted in a morning or afternoon time slot.



Legislative Affairs Bi-Weekly Meeting Agenda

December 22, 2022

10:00 – 10:30 am

Agenda

- 1. 118th Congress Leadership Update**
- 2. Hill Engagement**
 - a. Recap - COR Hearing FITARA/ Fed Cyber - December 15th
- 3. Legislation**
 - a. FY '23 Omnibus Recap
 - i. ONCD funded at FY '23 PBR of \$21.9 M (~4% increase over IIJA amount)
 - ii. New Authorities
 1. TikTok on government devices ban
 2. FDA cyber requirements for medical devices
 3. EBT Card fraud security requirements
 - b. 118th Congress ONCD Legislative Priorities
- 4. Staff Engagements**
 - a. Sen. Manchin & Workforce Team
 - b. Sen. Wyden - VEP
- 5. Other**
 - a. CISA Letter – Force Structure Assessment



FY '23 NDAA - Cyber Provisions of Interest

(b) (5)



FY '23 NDAA - Cyber Provisions of Interest

(b) (5)



FY '23 NDAA - Cyber Provisions of Interest

(b) (5)

Congress of the United States
House of Representatives
Washington, DC 20515–3202

December 16, 2022

The Honorable Alejandro Mayorkas
Secretary of Department of Homeland Security
Washington, DC 20528

Dear Secretary Mayorkas:

We write to convey our concern over the Department’s failure to submit the Cybersecurity and Infrastructure Security Agency (CISA) review and force structure assessment as required by law. The legislation requiring this review stemmed from a recommendation from the Cyberspace Solarium Commission¹ to strengthen CISA and received bipartisan support in Congress. We aim to better understand CISA’s current efforts to execute its mission, and how the Agency applies its personnel and resources to safeguard the American people from physical and cyber risk to the critical infrastructure that underpins our way of life.

As you know, the Department was mandated to conduct this comprehensive review of the ability of the Agency to fulfill its mission obligations, as well as a completion of a force structure assessment in the National Defense Authorization Act for Fiscal Year 2021 (FY21 NDAA).² The law states, “not later than one year after the date of the enactment of this Act, the Secretary of Homeland Security shall submit to Congress a report detailing the results of the assessment”. The deadline for submission to Congress was nearly a year ago – January 2022.

CISA’s mission is to lead the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure.³ As the nation’s risk advisor and lead federal civilian cybersecurity agency, CISA’s work is critically important to our country. Additionally, as the Department’s newest component agency, it is both appropriate and fundamental that you provide oversight over the growth, development, and execution of CISA’s relatively nascent authority in this space. As the Department overseeing CISA, submitting a baseline understanding of the ability of the Agency to fulfill “the missions of the Agency” and a “comprehensive force structure assessment of CISA” should be one of your highest priorities. These review efforts reflect back on the ability of the Department to effectively manage its components and are crucial to understanding CISA’s current ability to conduct its mission effectively, as well as its current and future resource needs.

Please detail the Department’s efforts to conduct this review and force assessment and the timeline for transmittal to Congress as soon as possible, but no later than January 3, 2023. Understanding CISA’s current ability to fulfill its mission and receiving a comprehensive review of the personnel and resources required to do so are absolutely paramount for Congressional oversight and the security of our Nation.

¹ Cyberspace Solarium Commission Report: <https://www.solarium.gov/report>

² William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021: <https://www.congress.gov/116/bills/hr6395/BILLS-116hr6395enr.pdf>

³ About CISA: <https://www.cisa.gov/about-cisa>

Congress of the United States
House of Representatives
Washington, DC 20515-3202

Sincerely,



John M. Katko
Ranking Member



Andrew R. Garbarino
Member of Congress



Mike Gallagher
Member of Congress

cc:

The Honorable Jennifer Easterly
Director of the Cybersecurity and Infrastructure Security Agency

The Honorable Robert Silvers
Undersecretary for Strategy, Policy, and Plans, DHS

The Honorable Iranga Kahangama
Assistant Secretary for Cyber, Infrastructure, Risk, and Resilience, DHS

The Honorable Christopher Inglis
National Cyber Director

Ms. Anne Neuberger
Deputy National Security Advisor for Cyber and Emerging Technology

Ms. Shalanda Young
Director of the Office of Management and Budget

SEC. 1745. CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY REVIEW.**(a) DHS REVIEW.—**

(1) **IN GENERAL.**—In order to strengthen the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, the Secretary of Homeland Security shall conduct a comprehensive review of the ability of the Agency to fulfill—

(A) the missions of the Agency; and

(B) the recommendations detailed in the report issued by the Cyberspace Solarium Commission under section 1652(k) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232).

Assessments.

(2) **ELEMENTS OF REVIEW.**—The review conducted under paragraph (1) shall include the following elements:

(A) An assessment of how additional budget resources could be used by the Cybersecurity and Infrastructure Security Agency for projects and programs that—

(i) support the national risk management mission;

(ii) support public and private-sector cybersecurity;

(iii) promote public-private integration; and

(iv) provide situational awareness of cybersecurity threats.

(B) A comprehensive force structure assessment of the Cybersecurity and Infrastructure Security Agency, including—

Determination.

(i) a determination of the appropriate size and composition of personnel to accomplish the mission of the Agency, as well as the recommendations detailed in the report issued by the Cyberspace Solarium Commission under section 1652(k) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232);

(ii) an assessment of whether existing personnel are appropriately matched to the prioritization of threats in the cyber domain and risks in critical infrastructure;

(iii) an assessment of whether the Agency has the appropriate personnel and resources to—

(I) perform risk assessments, threat hunting, incident response to support both private and public cybersecurity;

(II) carry out the responsibilities of the Agency related to the security of Federal information and Federal information systems; and

(III) carry out the critical infrastructure responsibilities of the Agency, including national risk management; and

(iv) an assessment of whether current structure, personnel, and resources of regional field offices are sufficient in fulfilling agency responsibilities and mission requirements.

Deadline.
Recommendations.

(3) **SUBMISSION OF REVIEW.**—Not later than one year after the date of the enactment of this Act, the Secretary of Homeland Security shall submit to Congress a report detailing the results of the assessments required under paragraph (1), including recommendations to address any identified gaps.

(b) **GENERAL SERVICES ADMINISTRATION REVIEW.**—

(1) IN GENERAL.—The Administrator of the General Services Administration shall—

(A) conduct a review of current Cybersecurity and Infrastructure Security Agency facilities and assess the suitability of such facilities to fully support current and projected mission requirements nationally and regionally; and

(B) make recommendations regarding resources needed to procure or build a new facility or augment existing facilities to ensure sufficient size and accommodations to fully support current and projected mission requirements, including the integration of personnel from the private sector and other departments and agencies. Recommendations.

(2) SUBMISSION OF REVIEW.—Not later than one year after the date of the enactment of this Act, the Administrator of the General Services Administration shall submit the review required under subsection (a) to— Deadline.

(A) the President;

(B) the Secretary of Homeland Security; and

(C) the Committee on Homeland Security and Governmental Affairs, the Committee on Appropriations, and the Committee on Environment and Public Work of the Senate, and the Committee on Homeland Security, the Committee on Appropriations, the Committee on Oversight and Reform, and the Committee on Transportation and Infrastructure of the House of Representatives.

SEC. 1746. REPORT ON ENABLING UNITED STATES CYBER COMMAND RESOURCE ALLOCATION.

(a) IN GENERAL.—Not later than April 15, 2021, the Secretary of Defense shall submit to the congressional defense committees a report detailing the actions the Secretary will undertake to implement clauses (ii) and (iii) of section 167b(d)(2) of title 10, United States Code, including actions to ensure that the Commander of United States Cyber Command has enhanced authority, direction, and control of the Cyber Operations Forces and the equipment budget that enables Cyber Operations Forces' operations and readiness, beginning with the budget to be submitted to Congress by the President under section 1105(a) of title 31, United States Code, for fiscal year 2024, and the budget justification materials for the Department of Defense to be submitted to Congress in support of such budget.

(b) ELEMENTS.—The report required by subsection (a) shall address the following items: Procedures.

(1) The procedures by which the Principal Cyber Advisor (PCA) will exercise authority, direction, and oversight over the Commander of United States Cyber Command, with respect to Cyber Operations Forces-peculiar equipment and resources.

(2) The procedures by which the Commander of United States Cyber Command will—

(A) prepare and submit to the Secretary program recommendations and budget proposals for Cyber Operations Forces and for other forces assigned to United States Cyber Command; and Recommendations.
Budget proposals.

(B) exercise authority, direction, and control over the expenditure of funds for—

BRIEFING MEMORANDUM

December 20, 2022

MEMORANDUM FOR THE NATIONAL CYBER DIRECTOR AND PRINCIPAL
DEPUTY NATIONAL CYBER DIRECTOR

FROM: Philip Stupak, Director, Federal Cybersecurity

THROUGH: Camille Stewart Gloster, Deputy National Cyber Director, Technology & Ecosystem

SUBJECT: Africa Leaders' Summit Readout – Cybersecurity Meeting

I. PURPOSE:

This memo conveys the details of a cybersecurity meeting held on the periphery of the Africa Leaders' Summit hosted by Cybastion and the Cybersecurity Alliance at Venable's Washington, DC offices.

II. BACKGROUND:

On December 13, 2022, Deputy National Cyber Director (DNCD) Stewart Gloster and Phil Stupak attended a multilateral meeting between U.S. Government (USG) representatives¹, French-speaking West African countries², and the private sector³ that focused on regional cybersecurity challenges.

III. DISCUSSION:

The discussion began with each country describing cybersecurity challenges before the conversation turned towards ongoing USG capacity building initiatives.

Regional Cybersecurity Challenges

Regionally, each country described progress on digitizing their society as a top concern.

- The **Benin** perspective tied digitization to improved tax collection, which supports all other domestic initiatives.
- **Burkina Faso** also highlighted the financing element but approached digitization from an intelligence perspective.

¹ ONCD, State Department (Bureau of Cyber space and Digital Policy), USAID, and Department of Commerce (NIST, Multilateral Development Bank Group)

² Burkina Faso, Benin, Cabo Verde, Cameroon, Republic of the Congo, and Niger

³ Cybastion, Venable, Cybersecurity Coalition, and Coris Bank

DRAFT//PRE-DECISIONAL
UNCLASSIFIED//FOR OFFICIAL USE ONLY

- **Niger** was heavily focused on workforce development given a population that is the youngest in the world (56.9% of the population is younger than 18 and 49.2% of the population is younger than 15) and highly decentralized.
- Other countries echoed the need for digital workforce development as a core element of cybersecurity capacity building. There was regional consensus on the need to partner with U.S. private sector companies to produce desired change.

One surprising comment came from Benin. Their delegation stated that they saw an increase in cyberattacks following the Russian invasion of Ukraine. This point was not elaborated on, but the traditional ruler of Benin, Oba Ewuare II, has been vocal on African impacts of the war and his hope that hostilities end.

USG Capacity Building

DNCD Stewart Gloster started the USG portion of the discussion by highlighting ONCD's willingness to be a partner especially on digital workforce development and zero trust. This seemed well received by the representatives. State Department's Bureau of Cyberspace and Digital Policy (CDP) broadly offered regional capacity building and training efforts, and tied the same to the *UN Framework on Responsible State Behavior in Cyberspace* while highlighting ongoing programs in Benin and Niger. Amy Mahn, NIST, offered assistance with standards through the French translation of the National Cyber Framework.

Danica Starks, Head of the Multilateral Development Bank Group, at the Department of Commerce provided an interesting briefing on the role of the World Bank within cybersecurity development. Ms. Starks' presentation focused on three key initiatives led by the World Bank:

- **Closing the digital connectivity gap.** Affordable mobile broadband (3G/4G) is particularly important to drive connectivity forward, though fiber optic connections are growing rapidly in main economic centers. Extending broadband to areas with no coverage presents a substantial economic challenge.
- **Investing in safe and open digital public infrastructure.** Digital public infrastructure comprise platforms hosted in data centers and clouds for digital identification, payments, data sharing, representing key elements for digital transactions including authentication of individuals and payments, and the flow of money and data. Only when such platforms are able to integrate and work together seamlessly and safely, can more sophisticated products and services be unlocked.
- **Helping countries access and use digital services.** Investments to improve connectivity and internet access along with DPIs offers leapfrogging opportunities to increase productivity and promises new solutions to long-standing problems.

She also offered the International Finance Corporation as a vehicle for bringing public-private partnerships to work on these three initiatives. Representatives were interested in this tool as a way to bring U.S. private sector companies into domestic projects.

Summary

The French-speaking West African countries shared a common desire for digital workforce development and capacity building. There is a strong interest in working with the White House, World Bank, and U.S. private sector companies. ONCD is well positioned to build a coherent position across multiple USG agencies and to explore leading a delegation in late FY 2023.

IV. NEXT STEPS

DNCD Stewart Gloster plans to engage with the World Bank and the African Development Bank to learn more as a next step prior to additional engagement with French-speaking West African countries.

**DRAFT//PRE-DECISIONAL
UNCLASSIFIED//FOR OFFICIAL USE ONLY**

December 20, 2022

**OFFICE OF THE NATIONAL CYBER DIRECTOR
EXECUTIVE SECRETARY**

Tracking

NUMBER: N/A
VERSION: v(1.2)
DATE: 15 December 2022

Coordination and Approval

PREPARED BY: Philip Stupak, (b) (6) (b) (6)
CLEARED BY: Camille Stewart Gloster, DNCD Technology and Ecosystem
Caroline Chang, Senior Advisor, ExecSec
Joe Scheidler, Special Advisor, ExecSec

Documents

ATTACHMENTS: Attendees

**DRAFT//PRE-DECISIONAL
UNCLASSIFIED//FOR OFFICIAL USE ONLY**

ATTACHMENT A: Attendees

International Government

- Michael Folane, Program Lead, PAYCR, Burkina Faso
- Wend-Panga Herman Ouedraogo, Technical Director, PAYCR, Burkina Faso
- Sekou Ouedraogo, Deputy Director of Intelligence, Burkina Faso
- Josue Toe, Administrative and Financial Head of Intelligence, Burkina Faso
- Mahamady Belem, Public Debt Director, Burkina Faso
- Colonel Pierre Ouedraogo, Head of Cybersecurity Center of Excellence, Burkina Faso
- Marc Andre Loko, CEO of ASIN, Benin
- Mahafous Osseni, Deputy Director, Port of Cotonou, Benin
- Ouanilo Medegan, Director of Security, Benin
- Henri Eyebe Ayissi, Minister of Domains, Cadaster and Land Affairs, Cameroon
- Lejeune Mbella, Minister of Foreign Affairs, Cameroon
- Alamine Ousmane Mey, Minister of Finance, Cameroon
- Mbarga Antagana, Minister of Commerce, Cameroon
- Sassou Nguesso, Minister of International Cooperation, Republic of the Congo
- Ibrahima Guimba, Head of Cybersecurity Agency, Niger
- Ahmat Jidoud, Minister of Finance, Niger

U.S. Government

- Camille Stewart Gloster, DNCD Technology & Ecosystem Security, ONCD, EOP
- Phil Stupak, Director of Federal Cybersecurity, ONCD, EOP
- Anne-Marie Mills, Senior Policy Advisor, CDP, Department of State
- Vanna Lavery, Cybersecurity & Digital Policy Office, CDP, Department of State
- Maurice Kent, Digital APEX Program Lead, USAID, Department of State
- Danica Starks, Head of Multilateral Development Bank Group, Department of Commerce
- Amy Mahn, International Policy Specialist, NIST, Department of Commerce
- Andrew Rollo, Vice President, China and Transformational Exports, Export-Import Bank

Industry

- Dr. Thierry Wandji, President and CEO, Cybastion
- Leila Ndiaye, SVP for Business Strategy & Government Affairs, Cybastion
- Andre Biyong, SVP of Operations, Cybastion
- Emana Shunnom, Senior Manager of Policy, Cybastion
- Alex Botting, Senior Director, Venable
- Tanvi Chopra, Cybersecurity Analyst, Venable
- Ari Schwartz, Coordinator, Cybersecurity Coalition

DRAFT//PRE-DECISIONAL
UNCLASSIFIED//FOR OFFICIAL USE ONLY

- Idrissa Nassa, Chairman, Coris Bank
- Stephane Tapsoba, Deputy Director for Burkina, Coris Bank

As of December 21, at 10:00 am



National Cyber Director

Daily Schedule

Thursday, December 22, 2022

Time	Topic	Location	Participants	
9:00-9:15 am	ONCD Daily Stand-Up	Virtual	ONCD Staff	
10:00-10:30 am	Bi-weekly Sync with Legislative Affairs	Virtual	ONCD Leg Affairs Team	1
12:30-1:15 pm	Internal Staff Discussion re: International Portfolio	Virtual	ONCD Staff; Decision Memo Enclosed	2
2:00-4:30 pm	POTUS Holiday Reception	The White House		
5:00-5:30 pm	Chief of Staff Close-out	EEOB 470 Virtual		
	Briefing Materials: Open-Source Software Security Initiative (OS3I)		From TES Team	3
	Briefing Memo: Hackers at the White House (HATWH)		From Stakeholder Engagement and National Cyber Teams	4
	Briefing Memo: Africa Leaders' Summit Readout		From Phil Stupak and Camille Stewart Gloster	5
	Space Executive Forum Participant List & Agenda		From ONCD Space Team	6



Principal Deputy National Cyber Director

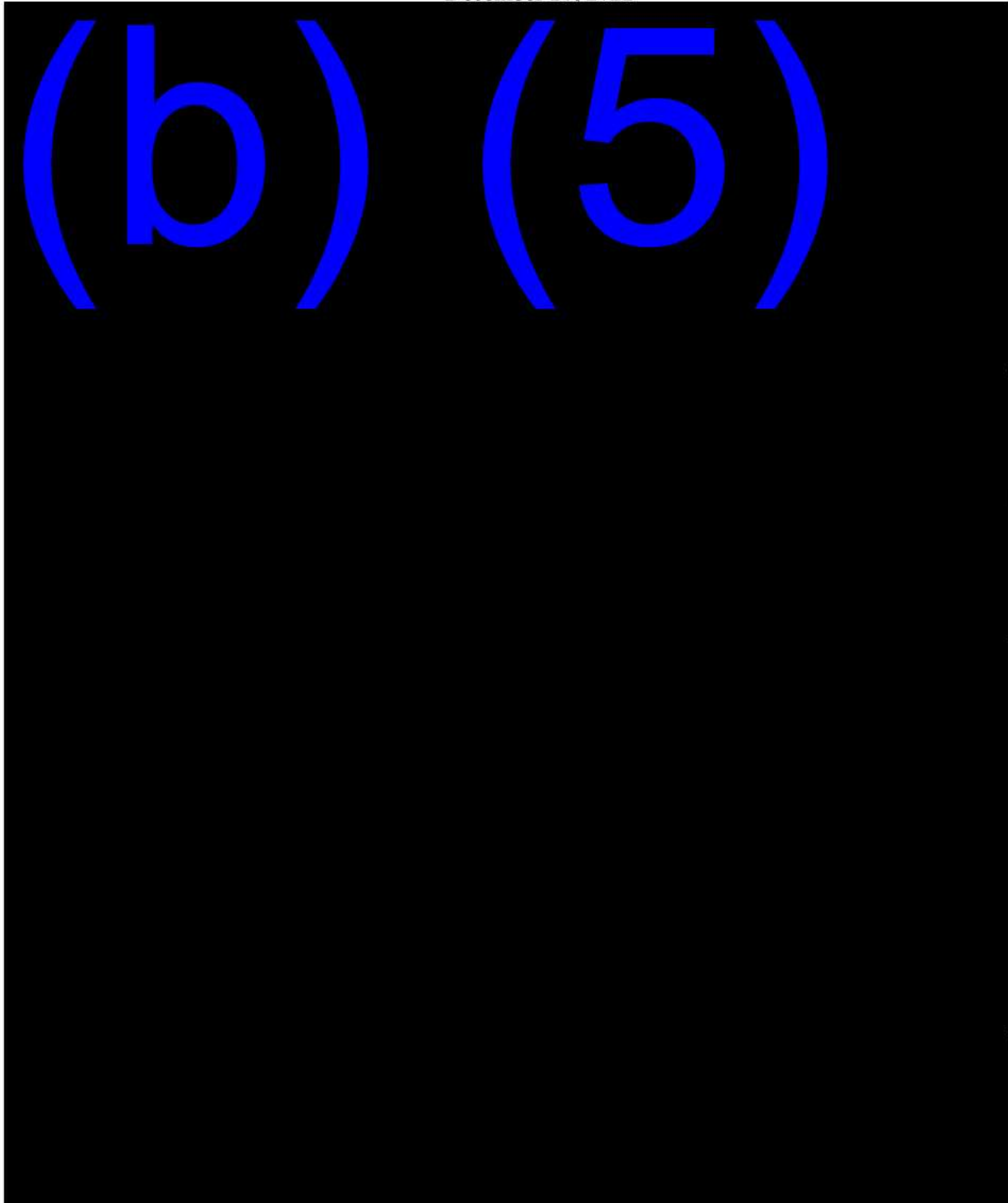
Daily Schedule

Thursday, December 22, 2022

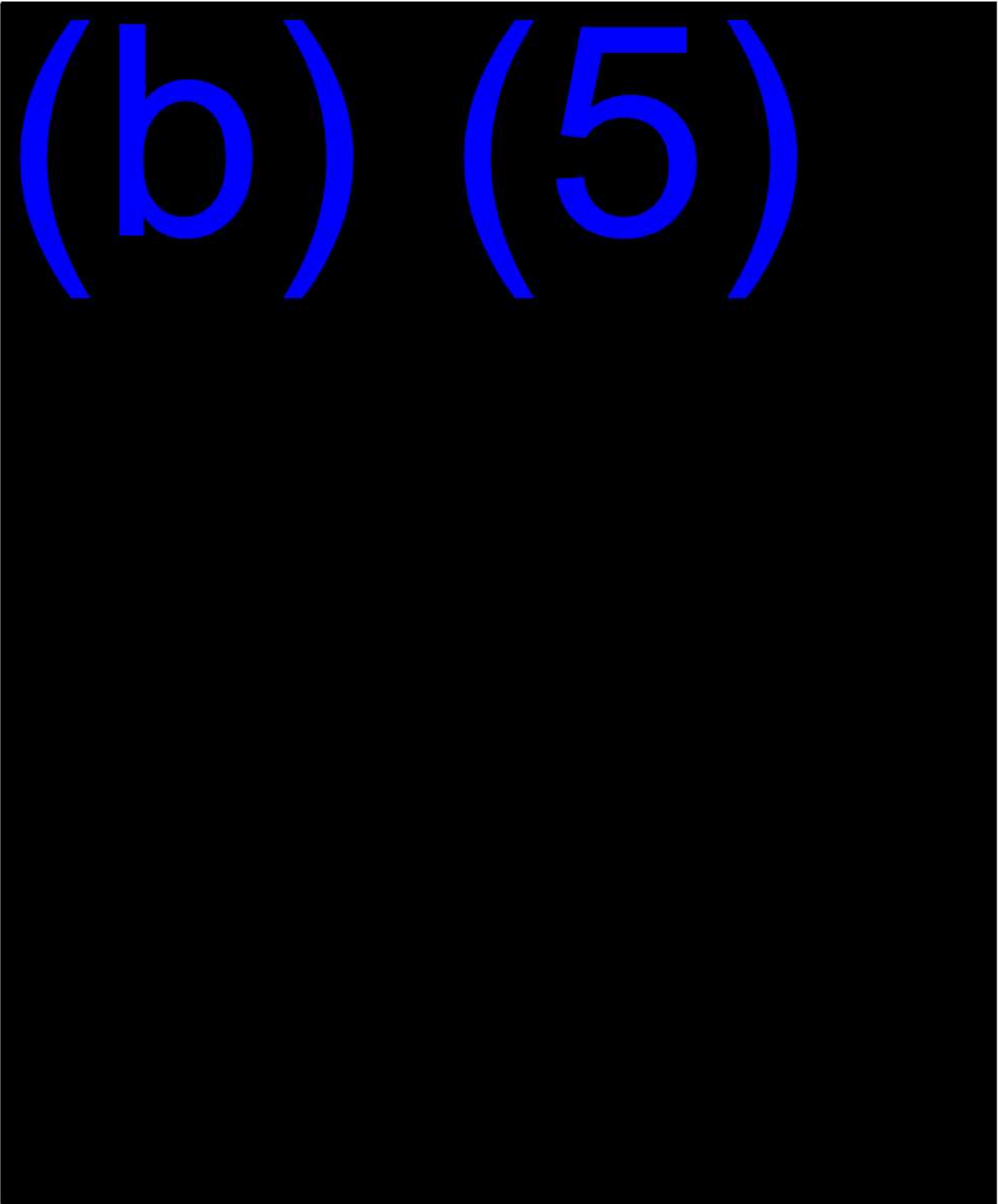
Time	Topic	Location	Participants	
9:00-9:15 am	ONCD Daily Stand-Up	Virtual	ONCD Staff	
10:00-10:30 am	Bi-weekly Sync w/ Legislative Affairs	Virtual	ONCD Leg Affairs Staff	1
12:30-1:15 pm	Internal Staff Discussion re: International Portfolio	Virtual	ONCD Staff; Decision Memo Enclosed	2
5:00-5:30 pm	Chief of Staff Close-out	EEOB 470 Virtual		
	Briefing Materials: Open-Source Software Security Initiative (OS3I)		From TES Team	3
	Briefing Memo: Hackers at the White House (HATWH)		From Stakeholder Engagement and National Cyber Teams	4
	Briefing Memo: Africa Leaders' Summit Readout		From Phil Stupak and Camille Stewart Gloster	5
	Space Executive Forum Participant List & Agenda		From ONCD Space Team	6

BRIEFING MEMORANDUM

December 20, 2022



(b) (5)



December 20, 2022

**OFFICE OF THE NATIONAL CYBER DIRECTOR
EXECUTIVE SECRETARY**

Tracking

NUMBER: 121922-002
VERSION: v (1.2)
DATE: 20 Dec 2022

Coordination and Approval

PREPARED BY: Jen Berlin, Assistant National Cyber Director for Stakeholder Engagement
Caitlin Clark, Assistant National Cyber Director Planning
Nick Leiserson, Assistant National Cyber Director Cyber Policy
Michael Morris, Assistant National Cyber Director Public Affairs
Jonathan Ring, Director, National Cybersecurity

CLEARED BY: Caroline Chang, Senior Advisor, ExecSec
Joe Scheidler, Special Advisor, ExecSec

Documents

ATTACHMENTS: N/A

**UNCLASSIFIED//FOR OFFICIAL USE ONLY
DISCUSSION DRAFT//PRE-DECISIONAL//DELIBERATIVE**

December 15, 2022

**DECISION MEMORANDUM FOR THE NATIONAL CYBER DIRECTOR AND
PRINCIPAL DEPUTY NATIONAL CYBER DIRECTOR**

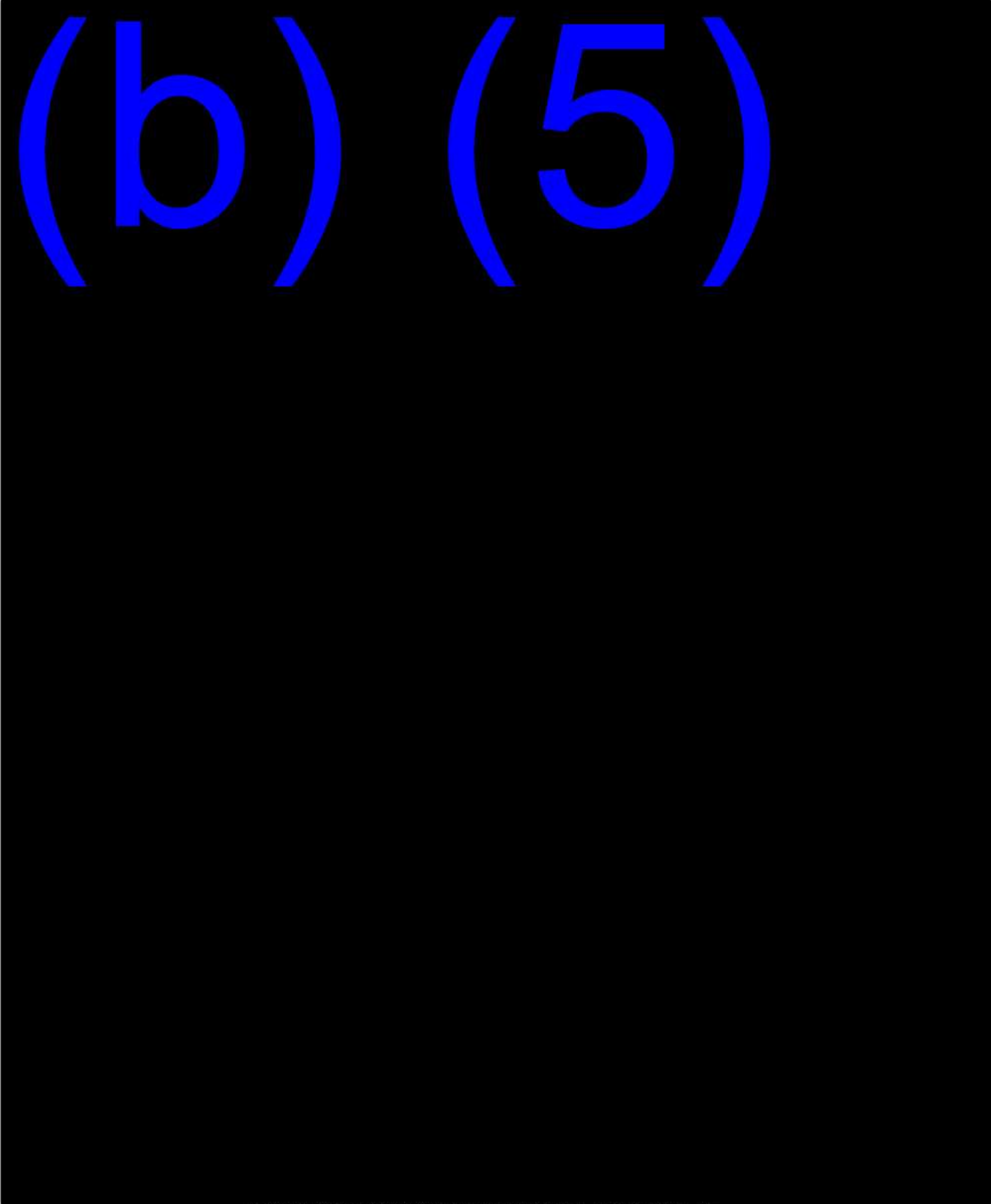
FROM: Harry Krejsa, ANCD Strategy and Research
Hannah Suh, Special Advisor

THROUGH: Michael Hochman, Chief of Staff

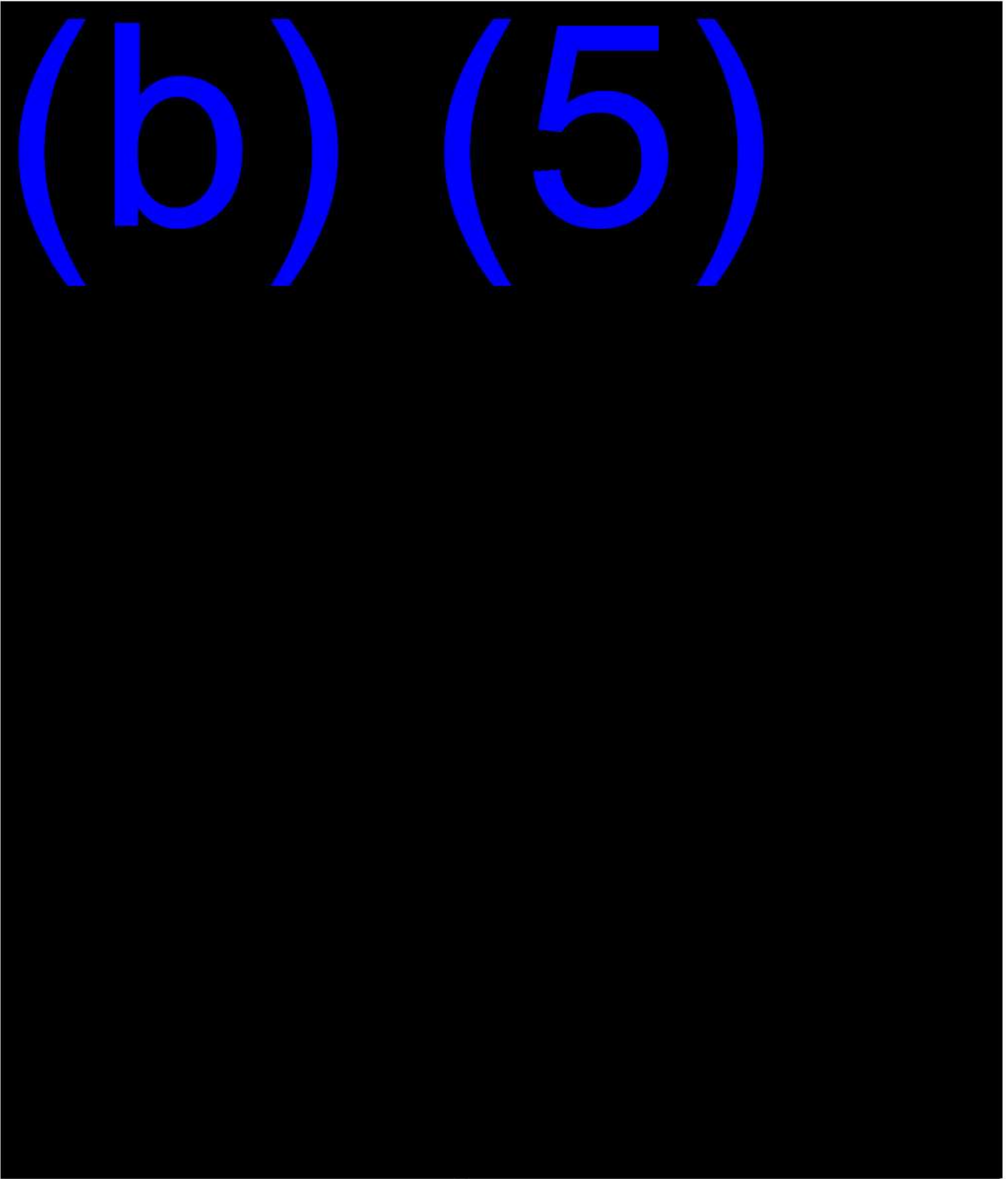
SUBJECT: ONCD International Engagements

(b) (5)

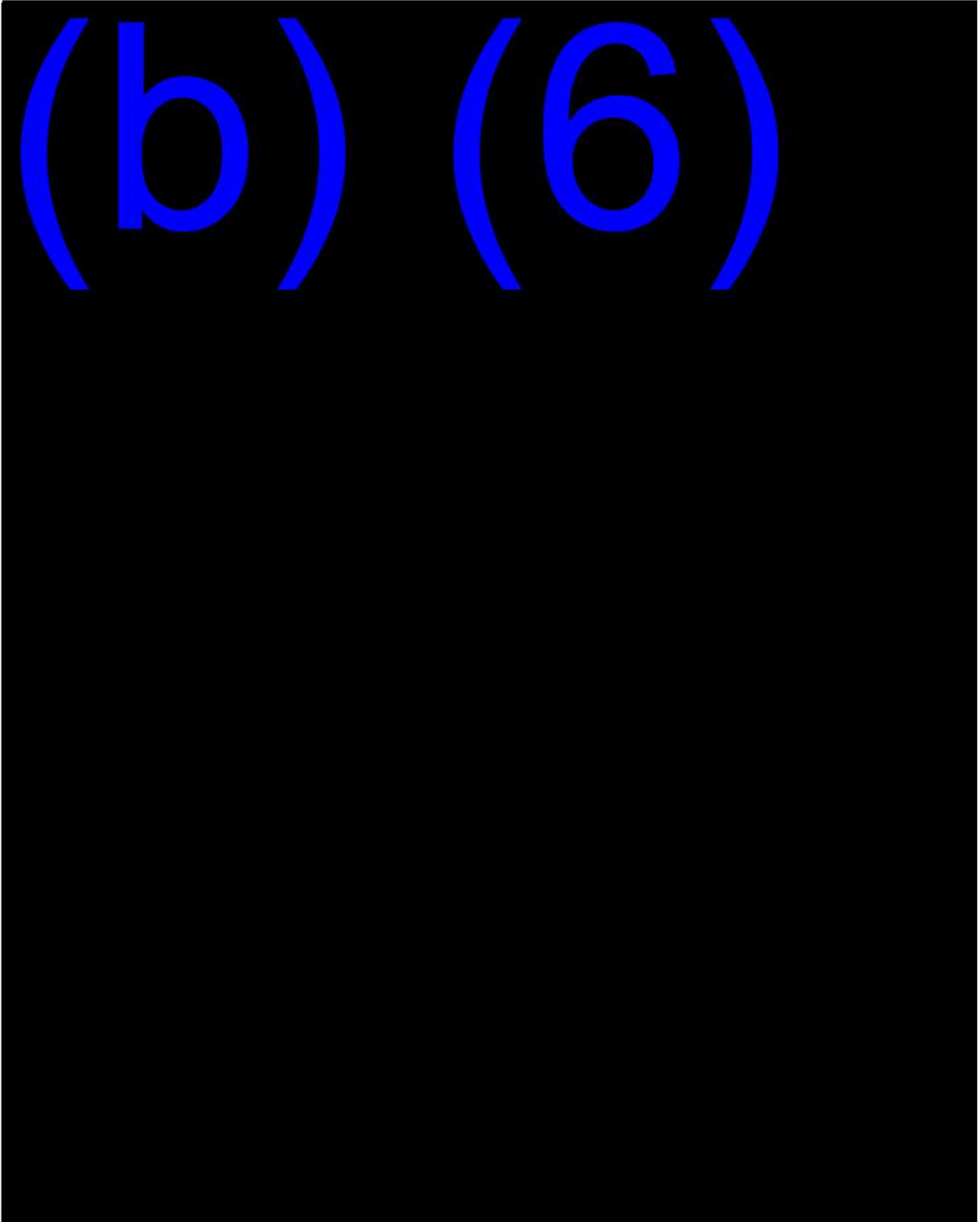
(b) (5)



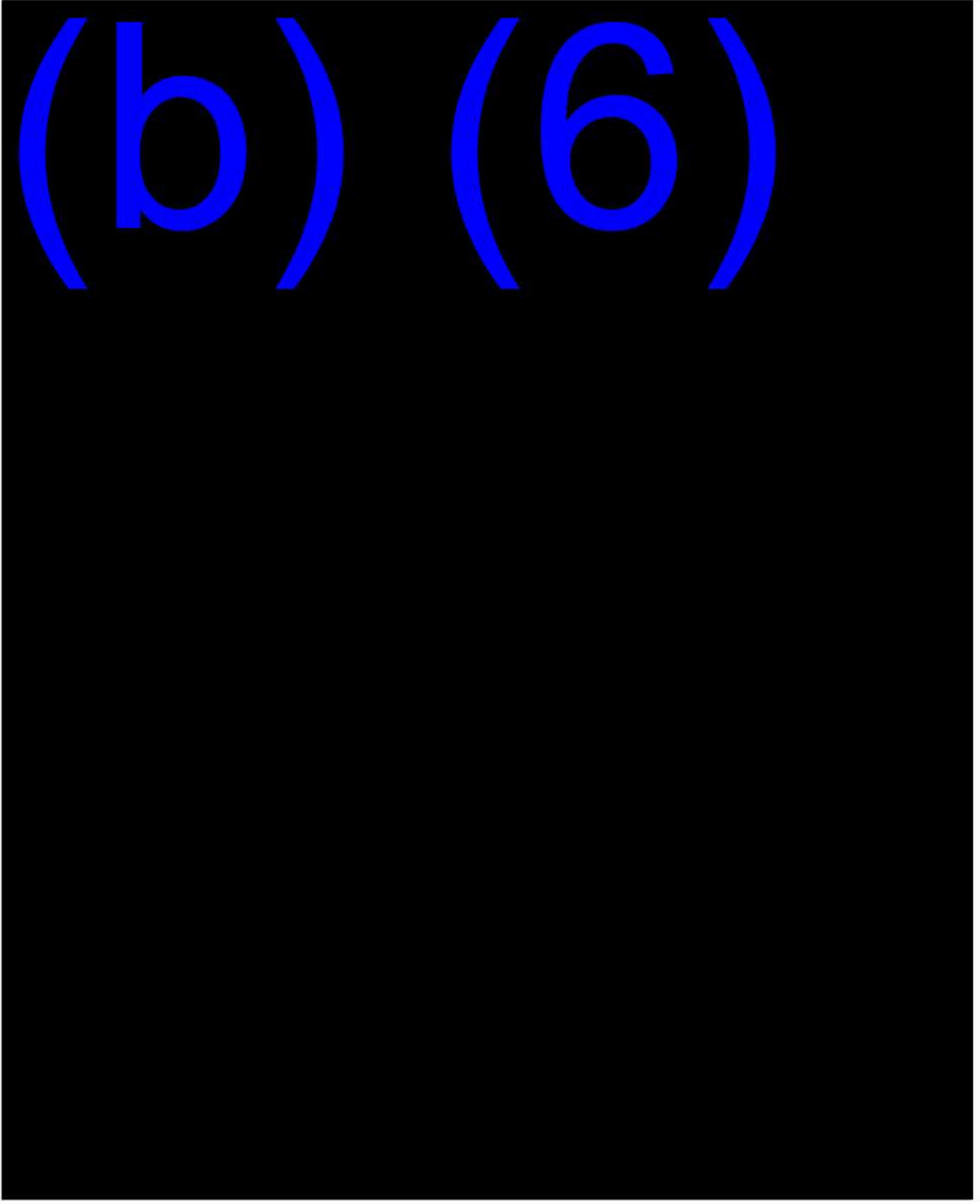
(b) (5)



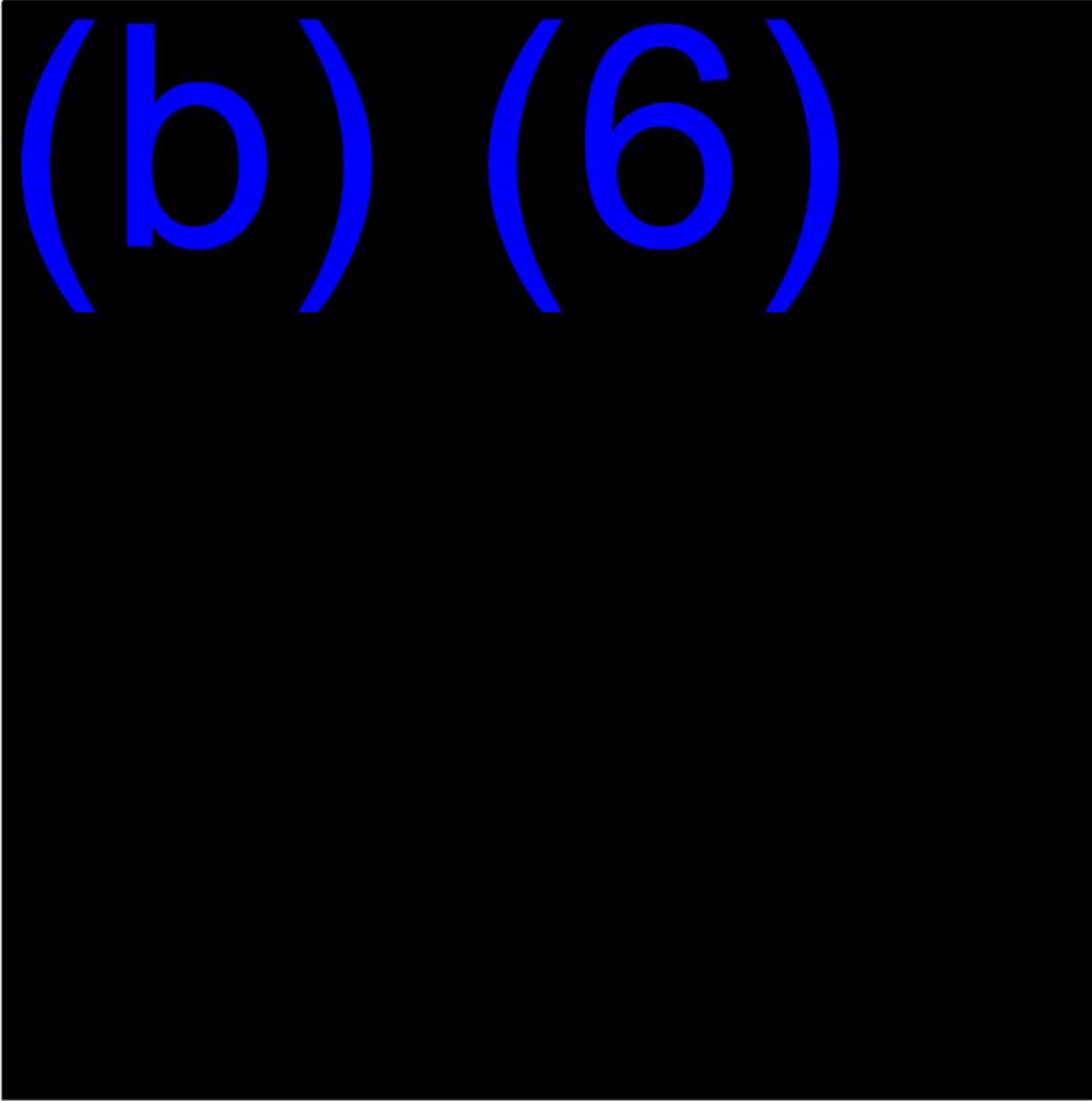
(b) (6)



(b) (6)



(b) (6)





December 15, 2022

OFFICE OF THE NATIONAL CYBER DIRECTOR DECISION

Approval and Coordination

1. **Scope and Impact.** ONCD and the interagency
2. **Coordinated and Approved.** This proposal was developed with all line divisions and has received clearance from the Deputies.

This decision memo was cleared by:

Caroline Chang, Senior Advisor, ExecSec
Michael Hochman, Chief of Staff

3. **Consulted.** N/A

Decision

Approve: _____	Approve as Amended: _____
Reject: _____	Discuss: _____
_____ JOHN C. INGLIS National Cyber Director Office of the National Cyber Director Executive Office of the President	_____ DATE

UNCLASSIFIED//FOR OFFICIAL USE ONLY
DISCUSSION DRAFT//PRE-DECISIONAL//DELIBERATIVE

Attachment A: Selections of Relevant Statutory Authorities

6 USC 1500 (National Cyber Director Act)

...

(c) Duties of the National Cyber Director

(1) In general

Subject to the authority, direction, and control of the President, the Director shall-

(A) serve as the principal advisor to the President on cybersecurity policy and strategy relating to the coordination of-

- (i) information security and data protection;
- (ii) programs and policies intended to improve the cybersecurity posture of the United States;
- (iii) efforts to understand and deter malicious cyber activity;
- (iv) efforts to increase the security of information and communications technology and services and to promote national supply chain risk management and vendor security;

(v) diplomatic and other efforts to develop norms and international consensus around responsible state behavior in cyberspace;

- (vi) awareness and adoption of emerging technology that may enhance, augment, or degrade the cybersecurity posture of the United States; and
- (vii) such other cybersecurity matters as the President considers appropriate;...

(2) Delegation of authority

(A) The Director may-

- (i) serve as the senior representative to any organization that the President may establish for the purpose of providing the President advice on cybersecurity;
- (ii) subject to subparagraph (B), be included as a participant in preparations for and, when appropriate, the execution of domestic and international summits and other international meetings at which cybersecurity is a major topic;**
- (iii) delegate any of the Director's functions, powers, and duties to such officers and employees of the Office as the Director considers appropriate; and
- (iv) authorize such successive re-delegations of such functions, powers, and duties to such officers and employees of the Office as the Director considers appropriate.

(B) In acting under subparagraph (A) (ii) in the case of a summit or a meeting with an international partner, the Director shall act in coordination with the Secretary of State...

FY23 NDAA Section 9502 (Cyber Diplomacy Act)

(a) In General.--Section 1 of the State Department Basic Authorities Act of 1956 (22 U.S.C. 2651a), is amended--

(1) by redesignating subsections (i) and (j) as subsection (j) and (k), respectively;

(2) by redesignating subsection (h) (as added by section 361(a)(1) of division FF of the Consolidated Appropriations Act, 2021 (Public Law 116-260)) as subsection (l); and

(3) by inserting after subsection (h) the following:

“(i) Bureau of Cyberspace and Digital Policy.--

“(1) In general.--There is established, within the Department of State, the Bureau of Cyberspace and Digital Policy (referred to in this subsection as the ‘Bureau’). The head of the Bureau shall have the rank and status of ambassador and shall be appointed by the President, by and with the advice and consent of the Senate.

UNCLASSIFIED//FOR OFFICIAL USE ONLY
DISCUSSION DRAFT//PRE-DECISIONAL//DELIBERATIVE

``(2) Duties.--

``(A) In general.--The head of the Bureau shall perform such duties and exercise such powers as the Secretary of State shall prescribe, including implementing the diplomatic and foreign policy aspects of the policy described in section 9501(a) of the Department of State Authorization Act of 2022.

``(B) Duties described.--The principal duties and responsibilities of the head of the Bureau shall, in furtherance of the diplomatic and foreign policy mission of the Department of State, be--

``(i) to serve as the principal cyberspace policy official within the senior management of the Department of State and as the advisor to the Secretary of State for cyberspace and digital issues;

``(ii) to lead, coordinate, and execute, in coordination with other relevant bureaus and offices, the Department of State's diplomatic cyberspace, and cybersecurity efforts (including efforts related to data privacy, data flows, internet governance, information and communications technology standards, and other issues that the Secretary has assigned to the Bureau);

``(iii) to coordinate with relevant Federal agencies and the Office of the National Cyber Director to ensure the diplomatic and foreign policy aspects of the cyber strategy in section 9501 of the Department of State Authorization Act of 2022 and any other subsequent strategy are implemented in a manner that is fully integrated with the broader strategy;

``(iv) to promote an open, interoperable, reliable, and secure information and communications technology infrastructure globally;

``(v) to represent the Secretary of State in interagency efforts to develop and advance Federal Government cyber priorities and activities, including efforts to develop credible national capabilities, strategies, and policies to deter and counter cyber adversaries, and carry out the purposes of title V of the Department of State Authorization Act of 2022;

``(vi) to engage civil society, the private sector, academia, and other public and private entities on relevant international cyberspace and international information and communications technology issues;

``(vii) to support United States Government efforts to uphold and further develop global deterrence frameworks for malicious cyber activity;

``(viii) to advise the Secretary of State and coordinate with foreign governments regarding responses to national security-level cyber incidents, including coordination on diplomatic response efforts to support allies and partners threatened by malicious cyber activity, in conjunction with members of the North Atlantic Treaty Organization and like-minded countries;

``(ix) to promote the building of foreign capacity relating to cyberspace policy priorities;

``(x) to promote an open, interoperable, reliable, and secure information and communications technology infrastructure globally and an open, interoperable, secure, and reliable internet governed by the multi-stakeholder model;

``(xi) to promote an international environment for technology investments and the internet that benefits

UNCLASSIFIED//FOR OFFICIAL USE ONLY
DISCUSSION DRAFT//PRE-DECISIONAL//DELIBERATIVE

United States economic and national security interests;
``(xii) to promote cross-border flow of data and
combat international initiatives seeking to impose
unreasonable requirements on United States businesses;
``(xiii) to promote international policies to
protect the integrity of United States and international
telecommunications infrastructure from foreign-based
threats, including cyber-enabled threats;
``(xiv) to lead engagement, in coordination with
relevant executive branch agencies, with foreign
governments on relevant international cyberspace,
cybersecurity, cybercrime, and digital economy issues
described in title V of the Department of State
Authorization Act of 2022;
``(xv) to promote international policies, in
coordination with the Department of Commerce, to secure
radio frequency spectrum in the best interests of the
United States;
``(xvi) to promote and protect the exercise of human
rights, including freedom of speech and religion,
through the internet;
``(xvii) to build capacity of United States
diplomatic officials to engage on cyberspace issues;
``(xviii) to encourage the development and adoption
by foreign countries of internationally recognized
standards, policies, and best practices;
``(xix) to support efforts by the Global Engagement
Center to counter cyber-enabled information operations
against the United States or its allies and partners;
and
``(xx) to conduct such other matters as the
Secretary of State may assign...

``(6) Coordination.--In implementing the duties prescribed under
paragraph (2), the head of the Bureau shall coordinate with the heads of
other Federal agencies, including the Department of Commerce, the
Department of Homeland Security, and other Federal agencies that the
National Cyber Director deems appropriate...

[Briefer's note on FY23 NDAA – The language referenced above passed the House on December 8, 2022, as part of the final NDAA negotiated between the House and Senate. The Senate is expected to take it up on or before December 16, 2022, after which it will go to the President for his signature. ONCD staff have very high confidence that this language will become law before the end of the calendar year.]

2022-12-22 NCD and PDNCD Briefing Book

From: "Chang, Caroline EOP/NCD" <(b) (6)>
To: "Inglis, Chris C. EOP/NCD" <(b) (6)>, "Walden, Kemba E. EOP/NCD" <(b) (6)>
Cc: DL ExecSec <(b) (6)>, "Hochman, Michael C. EOP/NCD" <(b) (6)>
Date: Wed, 21 Dec 2022 11:11:04 -0500
Attachments: 1. Mtg. Agenda Leg Affairs Bi-weekly.pdf (569.81 kB); 2. Decision Memo_Intl Engagement Strategy (Clean).pdf (345.35 kB); 3. Open Source Software Security Initiative.pdf (805.15 kB); 4. Briefing Memo - HATWH Event Concept.pdf (112.44 kB); 5. Briefing Memo - Africa Leaders Summit Readout.pdf (94.93 kB); 6. Space Executive Forum - Participant List and Agenda.pdf (268.56 kB); NCD - Daily Schedule.docx (91.45 kB); PDNCD - Daily Schedule.docx (91.09 kB)

Dear Chris and Kemba,

Please see attached your briefing book for tomorrow and the weekend. We are including a few of the papers we transmitted to you yesterday so you have all your holiday reading in one place. Please let us know if you have any questions.

1. Bi weekly Leg Affairs Sync Agenda + Read Ahead Materials
2. Decision Memo on International Strategy
3. Briefing Memo on Open Source Software Security Initiative
4. Briefing Memo on Hackers at the White House Event
5. Briefing Memo on Africa Leaders Summit Readout
6. Draft participant list and agenda for the Space Executive Forum
 - Please see the accompanying cover paragraph in the email enclosed

Best,
Caroline

Caroline Chang

Senior Advisor to NCD and ExecSec
Office of the National Cyber Director
Executive Office of the President

(b) (6)



Open Source Software Security Initiative (OS3I)

OS3I, an interagency working group, spent 2022 identifying risks and proposing strategic recommendations on securing the open-source software ecosystem. In 2023, OS3I will pursue a bold and ambitious implementation strategy that secures the software supply chain upstream and at scale. ONCD specifically will champion memory safety as its flagship open-source security issue in alignment with the National Cybersecurity Strategy.

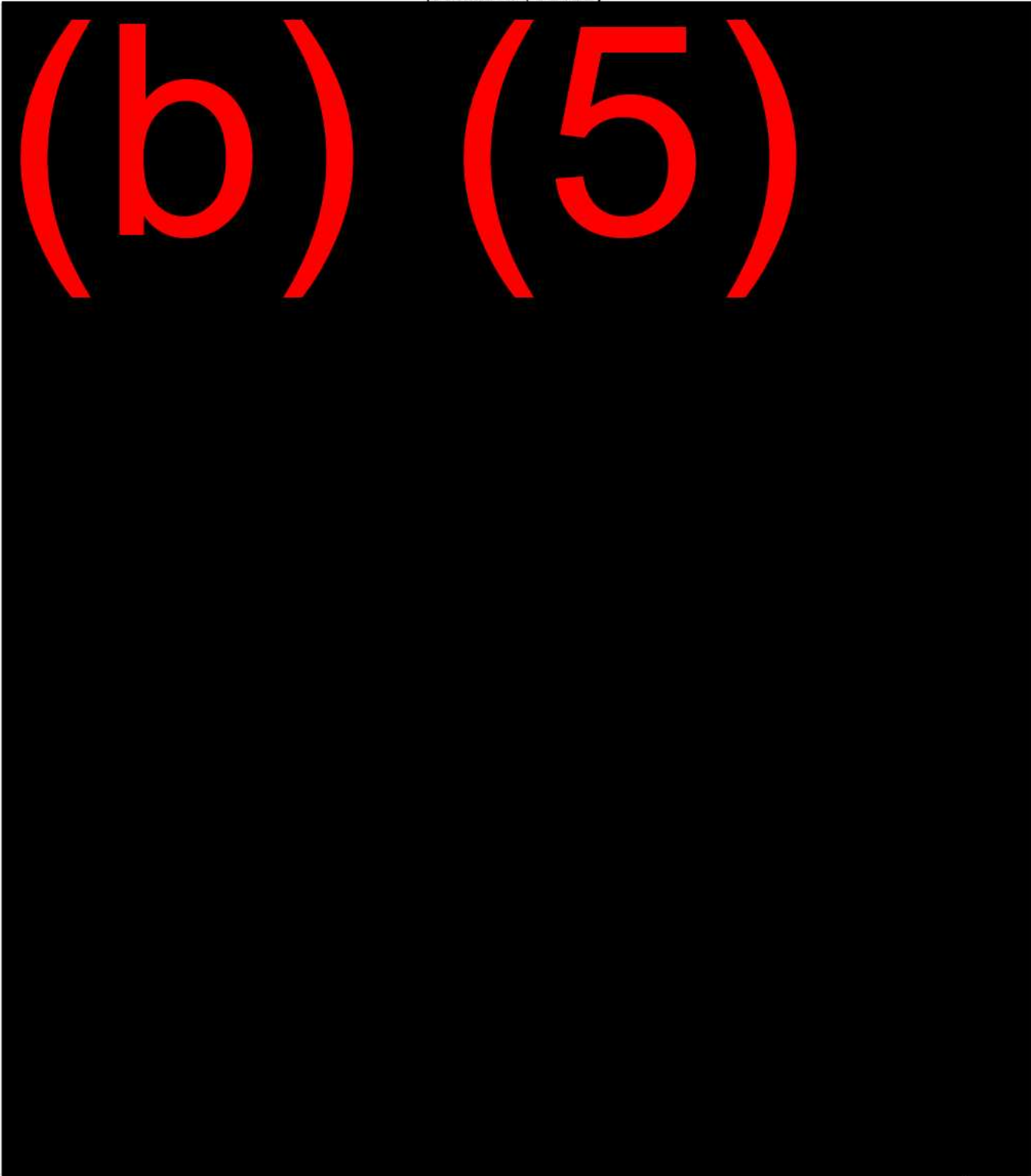
(b) (5)

Recommendations to Secure the Open-Source Software Ecosystem

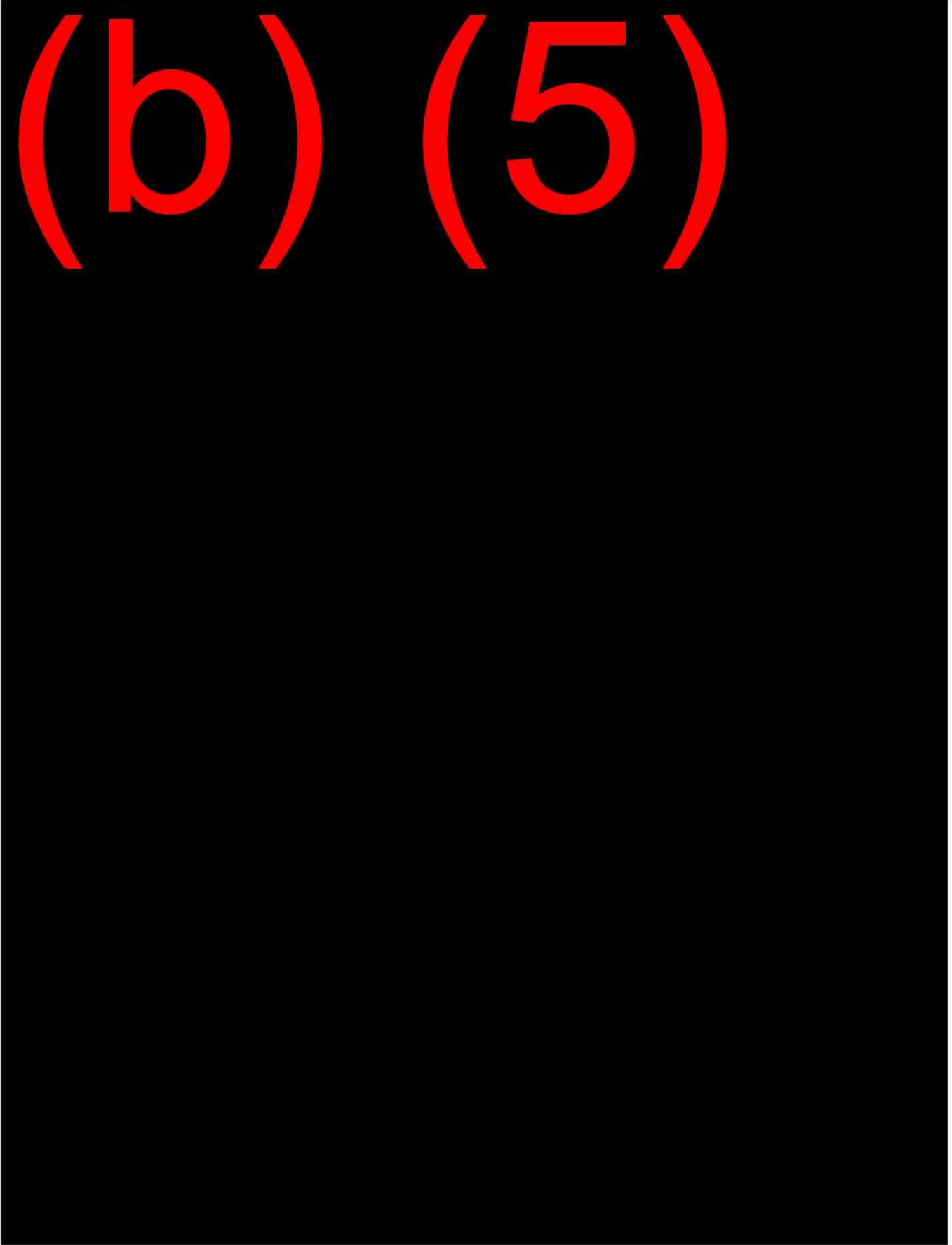
From the White House Open-Source Software Security Initiative

(Finalized Q4 2022)

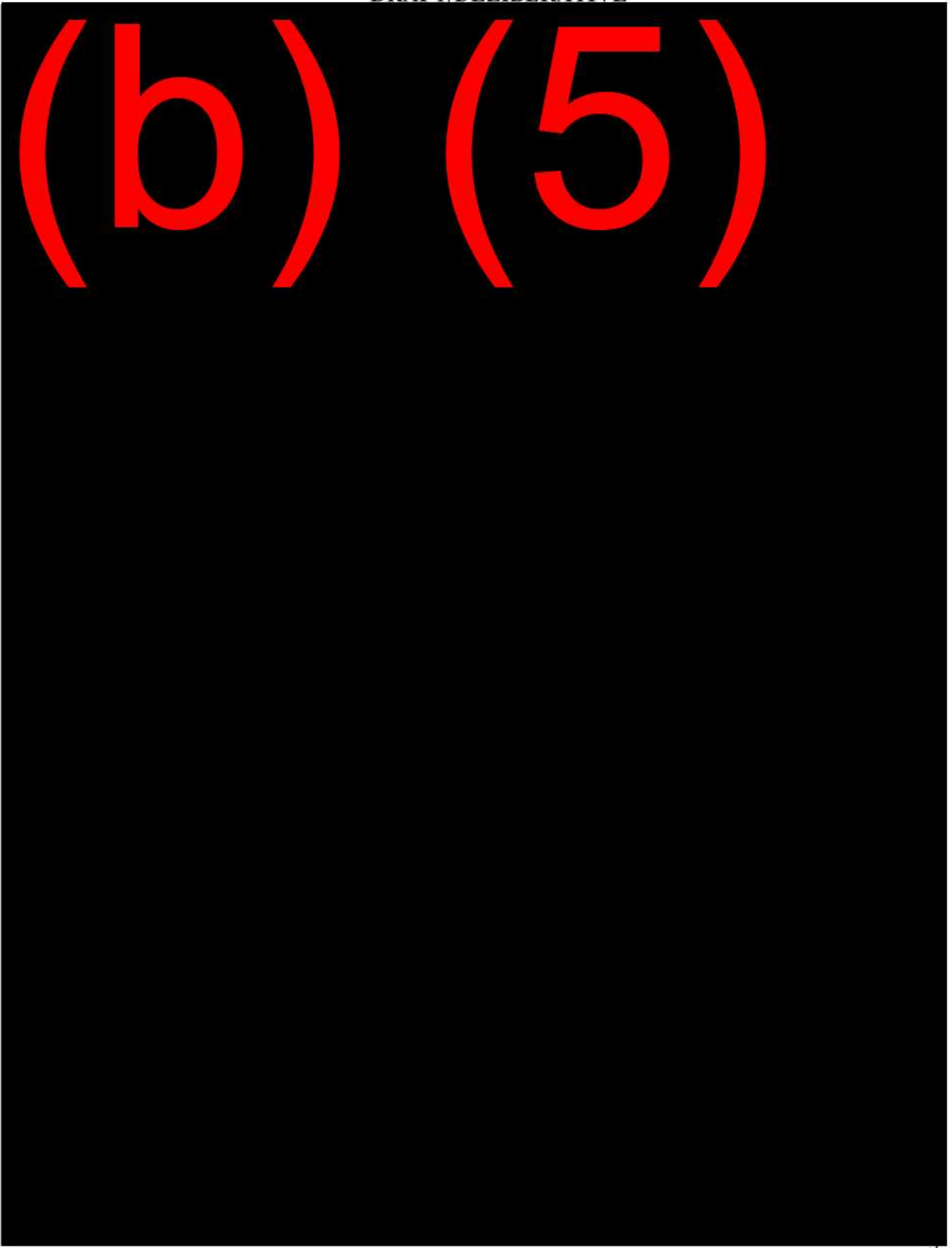
(b) (5)



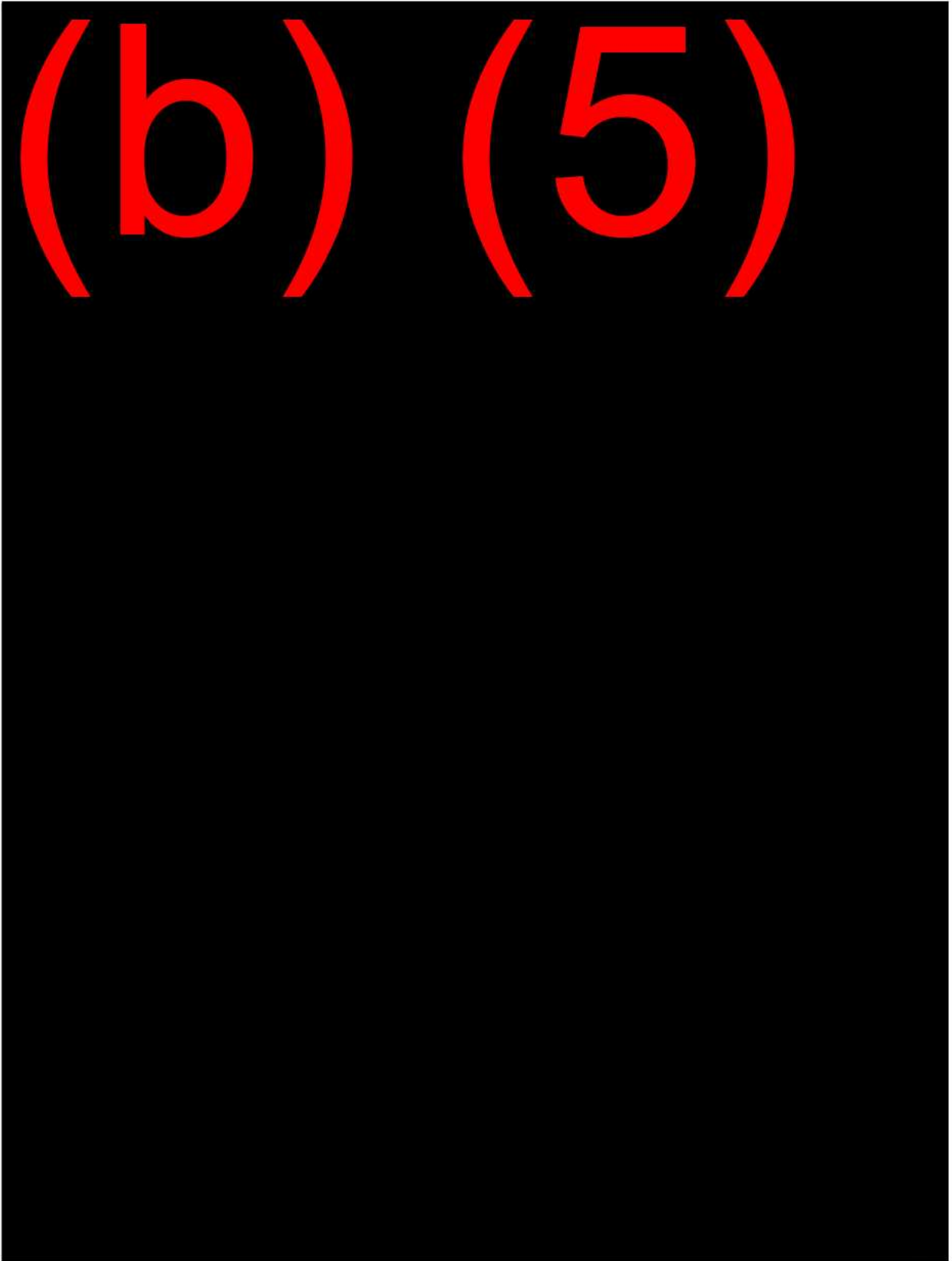
(b) (5)



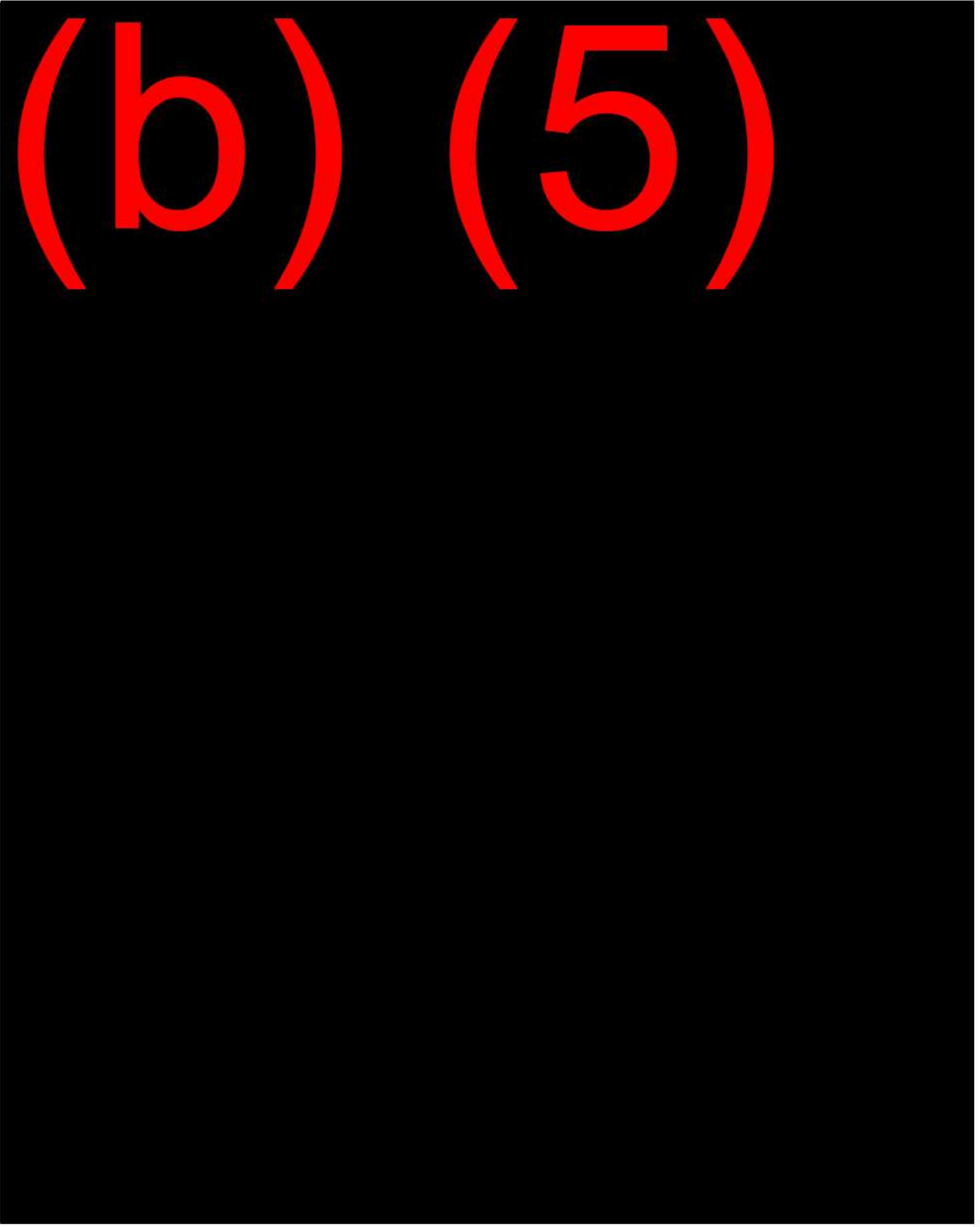
(b) (5)



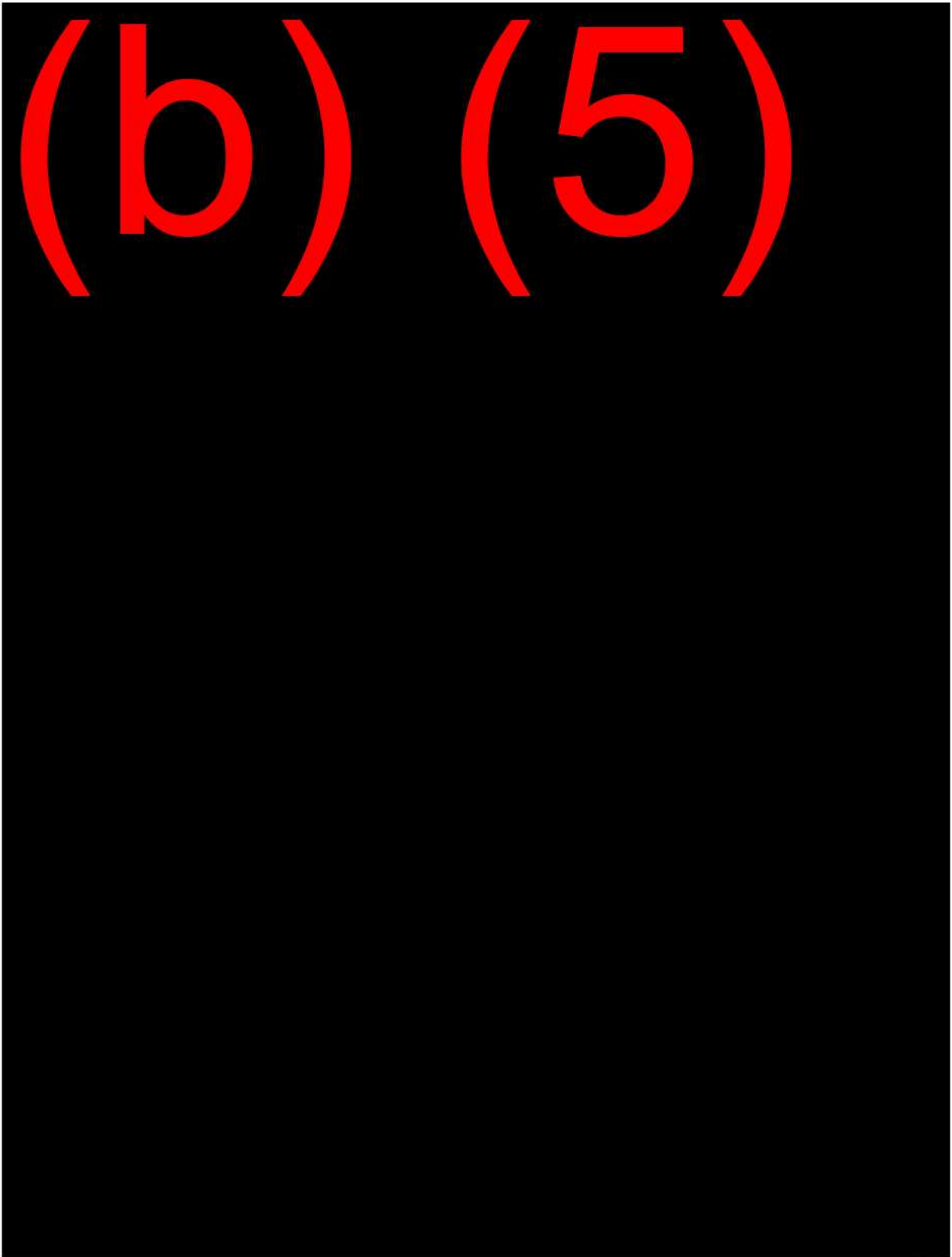
(b) (5)



(b) (5)



(b) (6)



(b) (5)

(b) (6)

(b) (5)

8

**MEMORANDUM FOR THE DEPUTY NATIONAL CYBER DIRECTOR
FOR TECHNOLOGY & ECOSYSTEM SECURITY**

FROM: Anjana Rajan
Assistant National Cyber Director
Technology Security

Seeyew Mo
Assistant National Cyber Director
Cyber Workforce

Eric Mill
Senior Advisor
Office of the Federal Chief Information Officer

Conrad Stosz
Policy Advisor
Office of the Federal Chief Information Officer

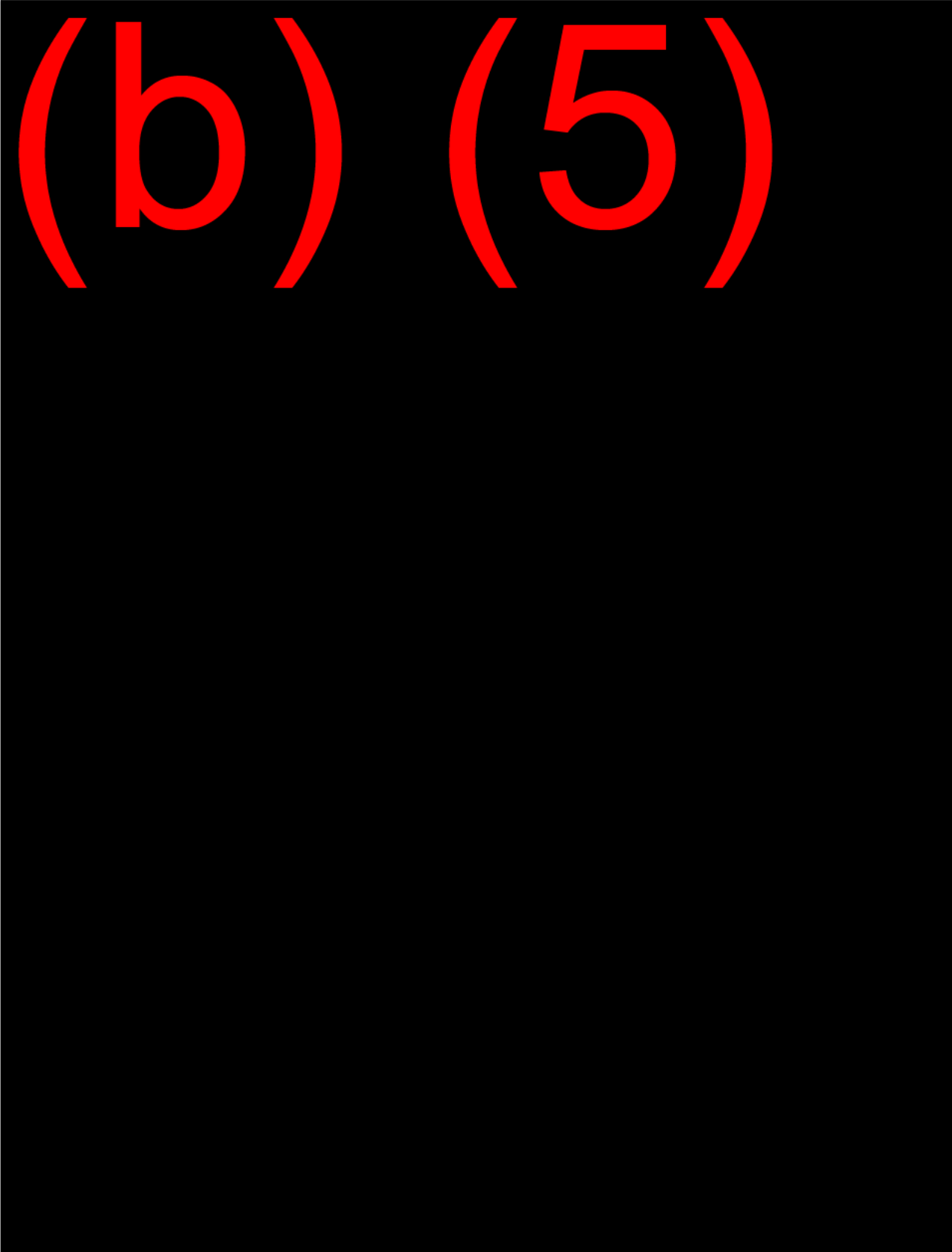
DATE: December 7, 2022

SUBJECT: Open-Source Software Security Initiative (OS3I):
2022 Strategic Recommendations (Phase I) & 2023 Implementation Initiatives (Phase II)

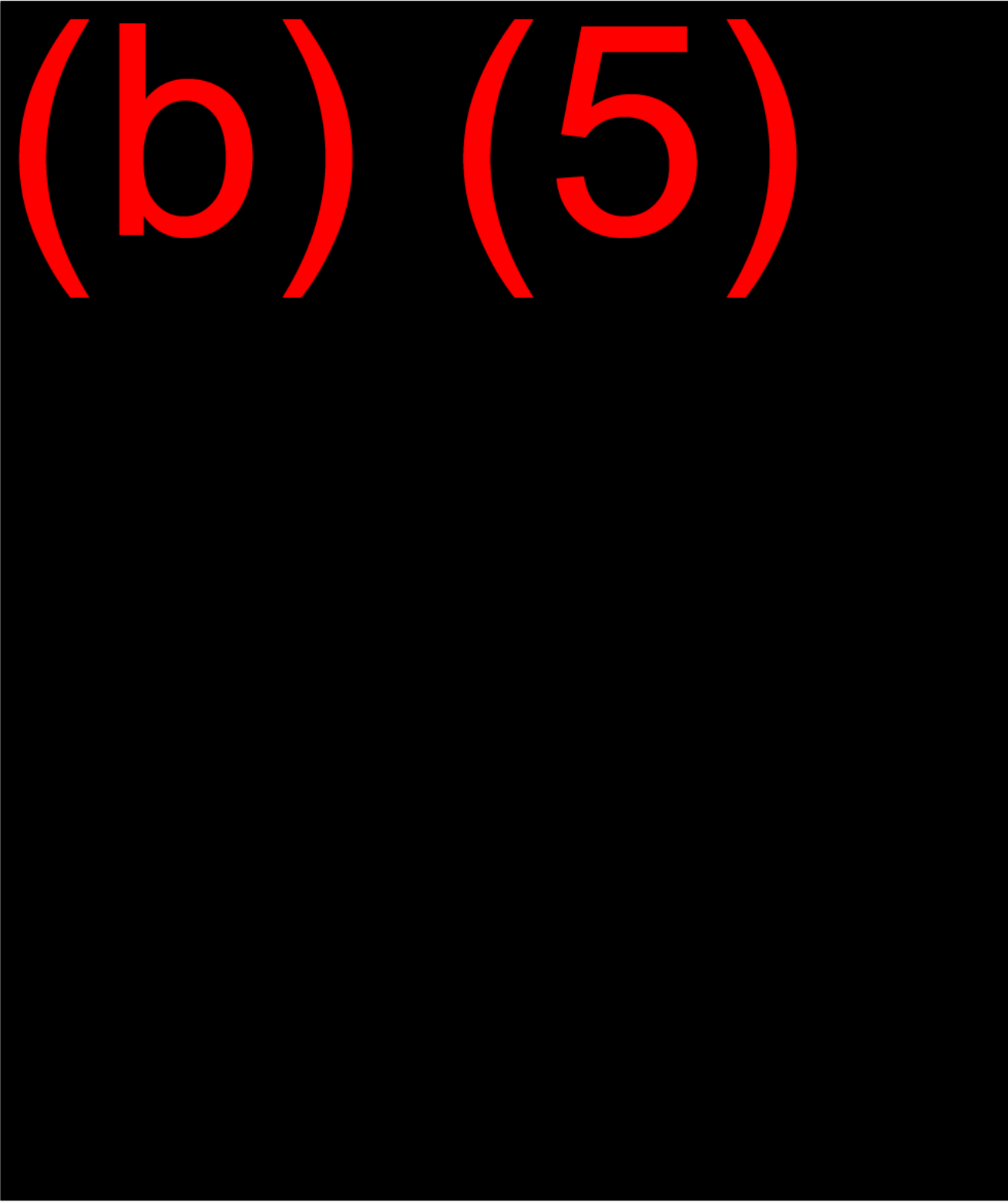
(b) (5)

(b) (5)

(b) (5)

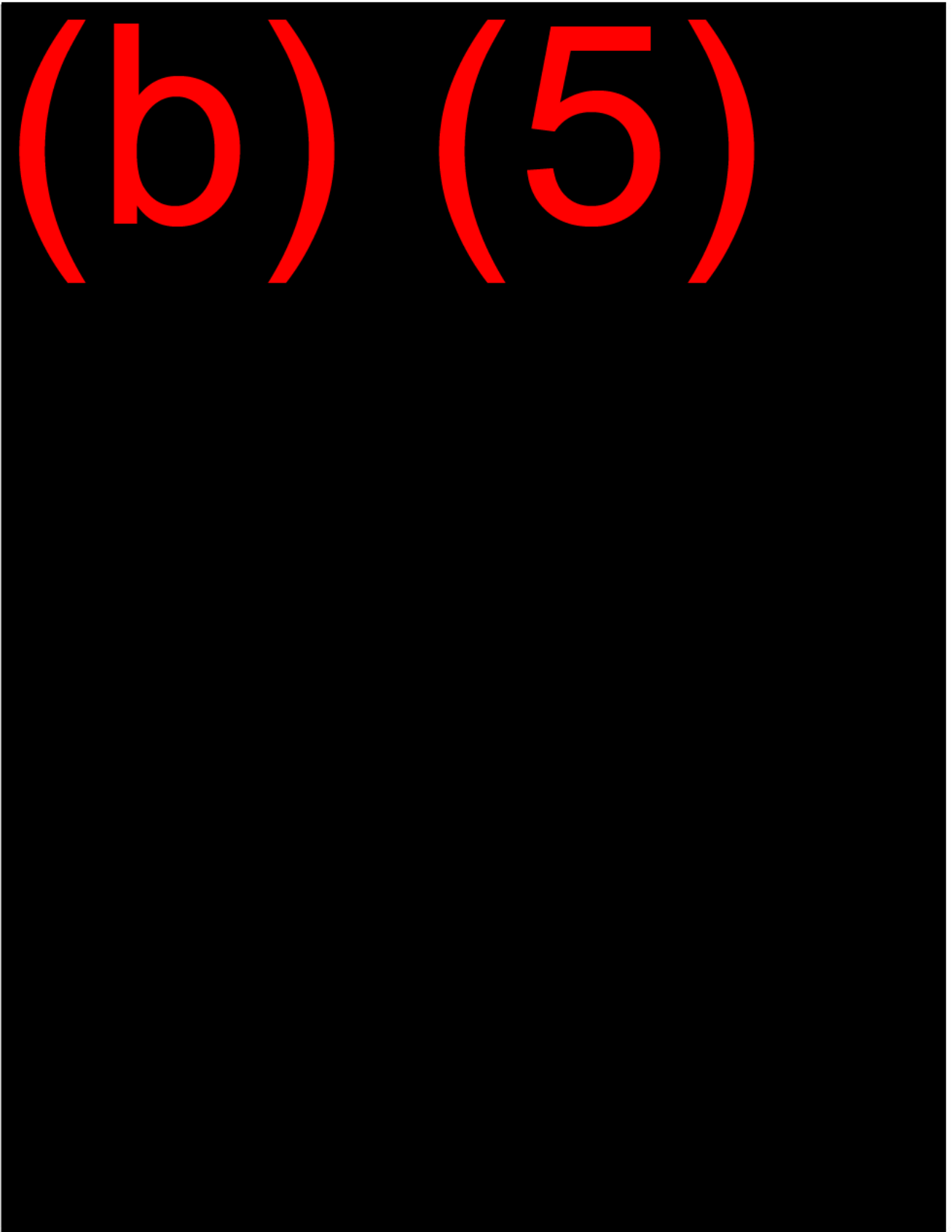


(b) (5)



(b) (5)

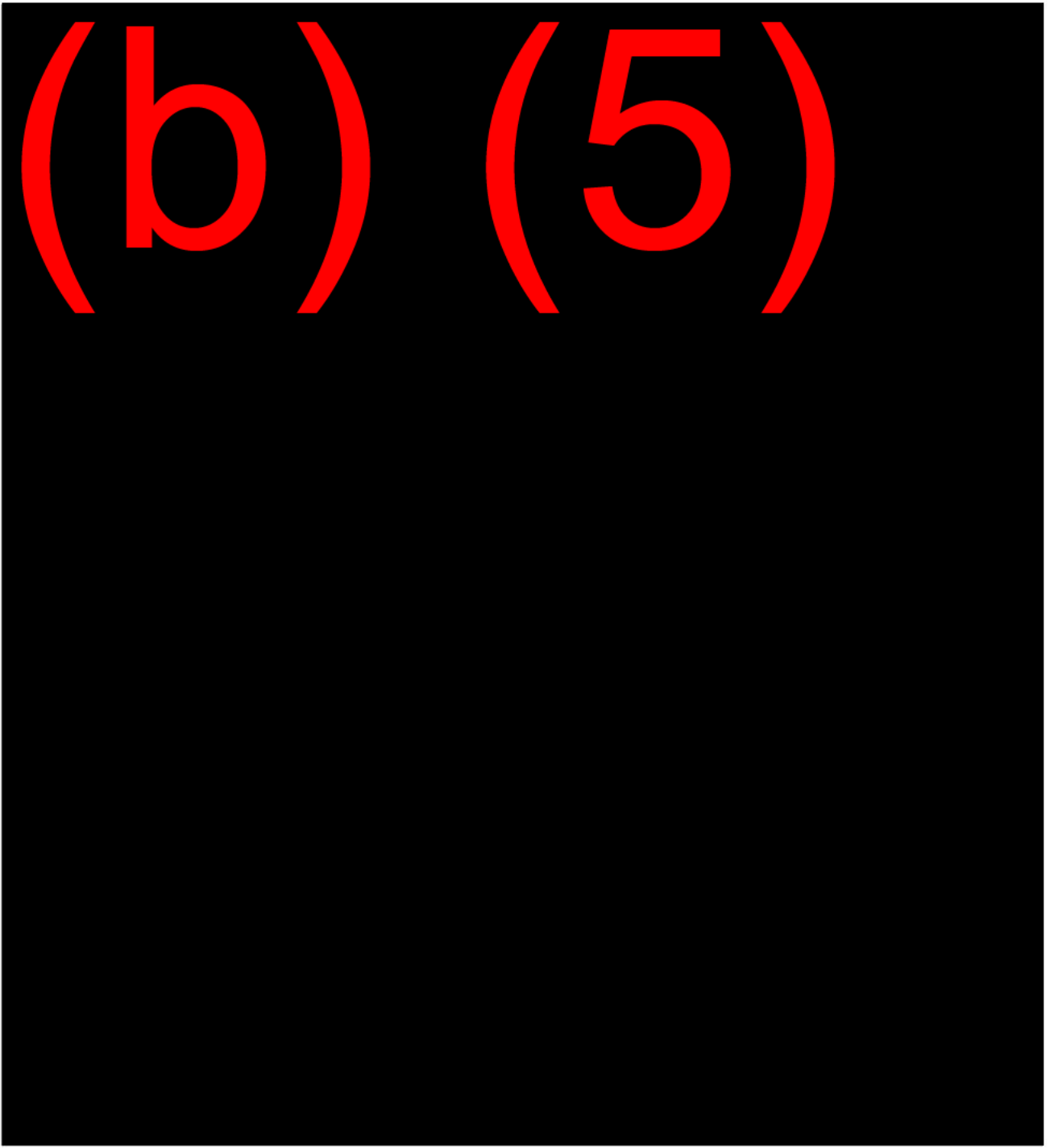
(b) (5)



(b) (5)

(b) (5)

(b) (5)



Approval and Coordination Decision

Attachment B: Open-Source Software Security Initiative – Executive Summary

Approve: _____ X Reject: _____	Approve as Amended: _____ Discuss: _____
CAMILLE STEWART Digitally signed by CAMILLE STEWART Date: 2022.12.19 10:36:17 -05'00' _____ CAMILLE STEWART GLOSTER Deputy National Cyber Director, TES Office of the National Cyber Director Executive Office of the President	_____ DATE



Principal Deputy National Cyber Director

Daily Schedule

Thursday, December 22, 2022

Time	Topic	Location	Participants	
9:00-9:15 am	ONCD Daily Stand-Up	Virtual	ONCD Staff	
10:00-10:30 am	Bi-weekly Sync w/ Legislative Affairs	Virtual	ONCD Leg Affairs Staff	1
12:30-1:15 pm	Internal Staff Discussion re: International Portfolio	Virtual	ONCD Staff; Decision Memo Enclosed	2
5:00-5:30 pm	Chief of Staff Close-out	EEOB 470 Virtual		
	Briefing Materials: Open-Source Software Security Initiative (OS3I)		From TES Team	3
	Briefing Memo: Hackers at the White House (HATWH)		From Stakeholder Engagement and National Cyber Teams	4
	Briefing Memo: Africa Leaders' Summit Readout		From Phil Stupak and Camille Stewart Gloster	5
	Space Executive Forum Participant List & Agenda		From ONCD Space Team	6

As of December 21, at 10:00 am



National Cyber Director

Daily Schedule

Thursday, December 22, 2022

Time	Topic	Location	Participants	
9:00-9:15 am	ONCD Daily Stand-Up	Virtual	ONCD Staff	
10:00-10:30 am	Bi-weekly Sync with Legislative Affairs	Virtual	ONCD Leg Affairs Team	1
12:30-1:15 pm	Internal Staff Discussion re: International Portfolio	Virtual	ONCD Staff; Decision Memo Enclosed	2
2:00-4:30 pm	POTUS Holiday Reception	The White House		
5:00-5:30 pm	Chief of Staff Close-out	EEOB 470 Virtual		
	Briefing Materials: Open-Source Software Security Initiative (OS3I)		From TES Team	3
	Briefing Memo: Hackers at the White House (HATWH)		From Stakeholder Engagement and National Cyber Teams	4
	Briefing Memo: Africa Leaders' Summit Readout		From Phil Stupak and Camille Stewart Gloster	5
	Space Executive Forum Participant List & Agenda		From ONCD Space Team	6



Legislative Affairs Bi-Weekly Meeting Agenda

December 22, 2022

10:00 – 10:30 am

Agenda

- 1. 118th Congress Leadership Update**
- 2. Hill Engagement**
 - a. Recap - COR Hearing FITARA/ Fed Cyber - December 15th
- 3. Legislation**
 - a. FY '23 Omnibus Recap
 - i. ONCD funded at FY '23 PBR of \$21.9 M (~4% increase over IIJA amount)
 - ii. New Authorities
 1. TikTok on government devices ban
 2. FDA cyber requirements for medical devices
 3. EBT Card fraud security requirements
 - b. 118th Congress ONCD Legislative Priorities
- 4. Staff Engagements**
 - a. Sen. Manchin & Workforce Team
 - b. Sen. Wyden - VEP
- 5. Other**
 - a. CISA Letter – Force Structure Assessment



FY '23 NDAA - Cyber Provisions of Interest

(b) (5)



FY '23 NDAA - Cyber Provisions of Interest

(b) (5)



FY '23 NDAA - Cyber Provisions of Interest

(b) (5)

Congress of the United States
House of Representatives
Washington, DC 20515–3202

December 16, 2022

The Honorable Alejandro Mayorkas
Secretary of Department of Homeland Security
Washington, DC 20528

Dear Secretary Mayorkas:

We write to convey our concern over the Department’s failure to submit the Cybersecurity and Infrastructure Security Agency (CISA) review and force structure assessment as required by law. The legislation requiring this review stemmed from a recommendation from the Cyberspace Solarium Commission¹ to strengthen CISA and received bipartisan support in Congress. We aim to better understand CISA’s current efforts to execute its mission, and how the Agency applies its personnel and resources to safeguard the American people from physical and cyber risk to the critical infrastructure that underpins our way of life.

As you know, the Department was mandated to conduct this comprehensive review of the ability of the Agency to fulfill its mission obligations, as well as a completion of a force structure assessment in the National Defense Authorization Act for Fiscal Year 2021 (FY21 NDAA).² The law states, “not later than one year after the date of the enactment of this Act, the Secretary of Homeland Security shall submit to Congress a report detailing the results of the assessment”. The deadline for submission to Congress was nearly a year ago – January 2022.

CISA’s mission is to lead the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure.³ As the nation’s risk advisor and lead federal civilian cybersecurity agency, CISA’s work is critically important to our country. Additionally, as the Department’s newest component agency, it is both appropriate and fundamental that you provide oversight over the growth, development, and execution of CISA’s relatively nascent authority in this space. As the Department overseeing CISA, submitting a baseline understanding of the ability of the Agency to fulfill “the missions of the Agency” and a “comprehensive force structure assessment of CISA” should be one of your highest priorities. These review efforts reflect back on the ability of the Department to effectively manage its components and are crucial to understanding CISA’s current ability to conduct its mission effectively, as well as its current and future resource needs.

Please detail the Department’s efforts to conduct this review and force assessment and the timeline for transmittal to Congress as soon as possible, but no later than January 3, 2023. Understanding CISA’s current ability to fulfill its mission and receiving a comprehensive review of the personnel and resources required to do so are absolutely paramount for Congressional oversight and the security of our Nation.

¹ Cyberspace Solarium Commission Report: <https://www.solarium.gov/report>

² William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021: <https://www.congress.gov/116/bills/hr6395/BILLS-116hr6395enr.pdf>

³ About CISA: <https://www.cisa.gov/about-cisa>

Congress of the United States
House of Representatives
Washington, DC 20515-3202

Sincerely,



John M. Katko
Ranking Member



Andrew R. Garbarino
Member of Congress



Mike Gallagher
Member of Congress

cc:

The Honorable Jennifer Easterly
Director of the Cybersecurity and Infrastructure Security Agency

The Honorable Robert Silvers
Undersecretary for Strategy, Policy, and Plans, DHS

The Honorable Iranga Kahangama
Assistant Secretary for Cyber, Infrastructure, Risk, and Resilience, DHS

The Honorable Christopher Inglis
National Cyber Director

Ms. Anne Neuberger
Deputy National Security Advisor for Cyber and Emerging Technology

Ms. Shalanda Young
Director of the Office of Management and Budget

SEC. 1745. CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY REVIEW.**(a) DHS REVIEW.—**

(1) **IN GENERAL.**—In order to strengthen the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, the Secretary of Homeland Security shall conduct a comprehensive review of the ability of the Agency to fulfill—

(A) the missions of the Agency; and

(B) the recommendations detailed in the report issued by the Cyberspace Solarium Commission under section 1652(k) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232).

Assessments.

(2) **ELEMENTS OF REVIEW.**—The review conducted under paragraph (1) shall include the following elements:

(A) An assessment of how additional budget resources could be used by the Cybersecurity and Infrastructure Security Agency for projects and programs that—

(i) support the national risk management mission;

(ii) support public and private-sector cybersecurity;

(iii) promote public-private integration; and

(iv) provide situational awareness of cybersecurity threats.

(B) A comprehensive force structure assessment of the Cybersecurity and Infrastructure Security Agency, including—

Determination.

(i) a determination of the appropriate size and composition of personnel to accomplish the mission of the Agency, as well as the recommendations detailed in the report issued by the Cyberspace Solarium Commission under section 1652(k) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232);

(ii) an assessment of whether existing personnel are appropriately matched to the prioritization of threats in the cyber domain and risks in critical infrastructure;

(iii) an assessment of whether the Agency has the appropriate personnel and resources to—

(I) perform risk assessments, threat hunting, incident response to support both private and public cybersecurity;

(II) carry out the responsibilities of the Agency related to the security of Federal information and Federal information systems; and

(III) carry out the critical infrastructure responsibilities of the Agency, including national risk management; and

(iv) an assessment of whether current structure, personnel, and resources of regional field offices are sufficient in fulfilling agency responsibilities and mission requirements.

Deadline.
Recommendations.

(3) **SUBMISSION OF REVIEW.**—Not later than one year after the date of the enactment of this Act, the Secretary of Homeland Security shall submit to Congress a report detailing the results of the assessments required under paragraph (1), including recommendations to address any identified gaps.

(b) **GENERAL SERVICES ADMINISTRATION REVIEW.**—

(1) IN GENERAL.—The Administrator of the General Services Administration shall—

(A) conduct a review of current Cybersecurity and Infrastructure Security Agency facilities and assess the suitability of such facilities to fully support current and projected mission requirements nationally and regionally; and

(B) make recommendations regarding resources needed to procure or build a new facility or augment existing facilities to ensure sufficient size and accommodations to fully support current and projected mission requirements, including the integration of personnel from the private sector and other departments and agencies. Recommendations.

(2) SUBMISSION OF REVIEW.—Not later than one year after the date of the enactment of this Act, the Administrator of the General Services Administration shall submit the review required under subsection (a) to— Deadline.

(A) the President;

(B) the Secretary of Homeland Security; and

(C) the Committee on Homeland Security and Governmental Affairs, the Committee on Appropriations, and the Committee on Environment and Public Work of the Senate, and the Committee on Homeland Security, the Committee on Appropriations, the Committee on Oversight and Reform, and the Committee on Transportation and Infrastructure of the House of Representatives.

SEC. 1746. REPORT ON ENABLING UNITED STATES CYBER COMMAND RESOURCE ALLOCATION.

(a) IN GENERAL.—Not later than April 15, 2021, the Secretary of Defense shall submit to the congressional defense committees a report detailing the actions the Secretary will undertake to implement clauses (ii) and (iii) of section 167b(d)(2) of title 10, United States Code, including actions to ensure that the Commander of United States Cyber Command has enhanced authority, direction, and control of the Cyber Operations Forces and the equipment budget that enables Cyber Operations Forces' operations and readiness, beginning with the budget to be submitted to Congress by the President under section 1105(a) of title 31, United States Code, for fiscal year 2024, and the budget justification materials for the Department of Defense to be submitted to Congress in support of such budget.

(b) ELEMENTS.—The report required by subsection (a) shall address the following items: Procedures.

(1) The procedures by which the Principal Cyber Advisor (PCA) will exercise authority, direction, and oversight over the Commander of United States Cyber Command, with respect to Cyber Operations Forces-peculiar equipment and resources.

(2) The procedures by which the Commander of United States Cyber Command will—

(A) prepare and submit to the Secretary program recommendations and budget proposals for Cyber Operations Forces and for other forces assigned to United States Cyber Command; and Recommendations.
Budget proposals.

(B) exercise authority, direction, and control over the expenditure of funds for—

Chang, Caroline EOP/NCD

From: Rajan, Anjana EOP/NCD
Sent: Tuesday, December 20, 2022 4:15 PM
To: Chang, Caroline EOP/NCD
Cc: Leiserson, Nick J. EOP/NCD; Williams, Lauryn D. EOP/NCD; Simms, Tanya L. EOP/NCD; Krejsa, Harry H. EOP/NCD; Scott, Brian C. EOP/NCD; Corell, Joyce E. EOP/NCD; Berlin, Jen S. EOP/NCD
Subject: [for NCD/PDNCD] Space Forum - Proposed Attendee List and Agenda
Attachments: Space Executive Forum - Participant List & Agenda.docx

Hi Caroline,

Linked and attached is our due out for Chris and Kemba on the [proposed attendees and agenda for the Space Forum](#). I've included a paragraph to include with this deliverable. Please let us know if you need anything from us on this!

Warmly,
Anjana

--

Dear Chris and Kemba,

Pursuant to our meeting last Tuesday, we have put together a draft attendee list and draft agenda. We look forward to hearing your comments. Our next step will be to begin socializing this with our interagency partners. We look forward to briefing you in the new year about our SPD-5 implementation plan and our progress on the Space Forum.

Thanks,
Space Team

--

Anjana Rajan
Assistant National Cyber Director, Technology Security
Office of the National Cyber Director

(b) (6) | (b) (6)

**Space Executive Forum
Proposed Participant List & Agenda**

Government		
At the table	• Chris Inglis • Kemba Walden • Kamala Harris • Bill Nelson • Chirag Parikh • Lloyd Austin/Kathleen Hicks • Avril Haines/Dr. Stacey Dixon • Gina Raimondo/Don Graves* • Alejandro Mayorkas/Jen Easterly • Anne Neuberger • Cara Abercrombie • Rob Joyce	• National Cyber Director • Principal Deputy National Cyber Director • VPOTUS, Chair, National Space Council • Administrator, NASA • Executive Secretary, National Space Council • Secretary/Deputy Secretary of Defense • Director for National Intelligence/PDDNI • Secretary/Deputy Secretary of Commerce • Secretary of DHS/CISA Director • NSC Deputy National Security Advisor for Cyber and Emerging Technology • Deputy Assistant to POTUS and defense/arms control policy coordinator • NSA
Observers		• Office of Space Commerce • USAF • USD(P)/ASD(Space Policy) • Made in America Office • FCC • NIST
Industry		
At the table	• Gwynne Shotwell* • Mark Dankberg* • Rob Meyerson* • Tory Bruno* • Roy Azevedo* • Kathy Warden* • Alex Karp* • Andy Jassy* • Tim Ellis * • David Ulevitch* • Trae Stephens*	• SpaceX, President & COO • ViaSat, CEO • Blue Origin, President • ULA, CEO • Raytheon Intel & Space, President • Northrup Grumman, President & CEO • Palantir, CEO • AWS, President & CEO • Relativity Space, CEO • a16z, GP American Dynamism • Founders Fund, GP
Observers		• Space ISAC • ACM/IEEE • JPL

* Threat Briefing Participant

Draft Agenda

- Intelligence Threat Briefing (1'50")
- Transition (0'10")
- Opening Remarks – USG (0'20")
- Discussion – all (1'05")
 - SPD-5 Implementation Plan Pillars
- Closing remarks/summary – NCD/VPOTUS (0'05")
- [Press gaggle – VPOTUS/NCD (0'15")]
- [Reception (1'15")]

Total Time: 3'30" (sans press gaggle and reception.) Can be hosted in a morning or afternoon time slot.

BRIEFING MEMORANDUM

December 20, 2022

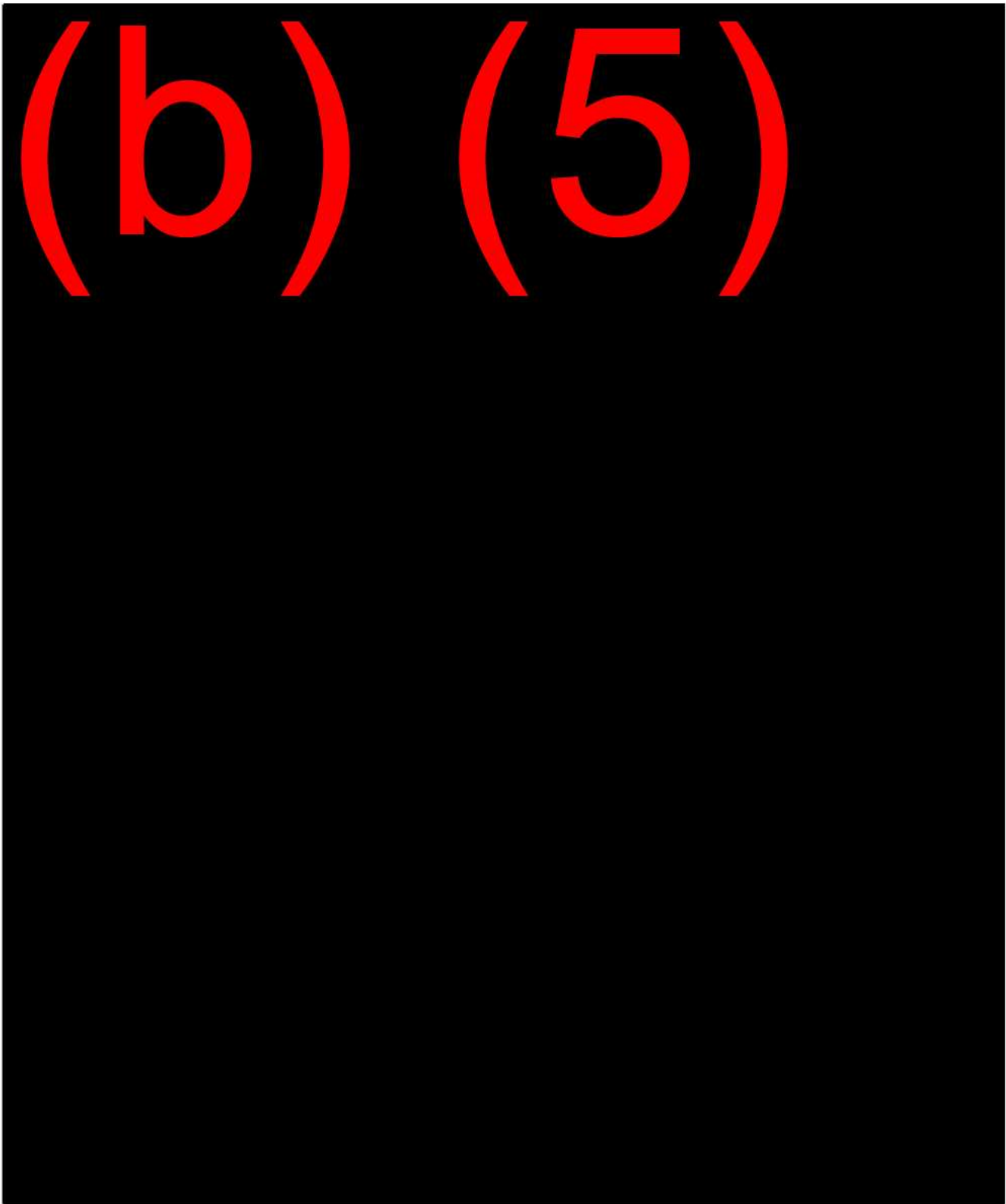
MEMORANDUM FOR THE NATIONAL CYBER DIRECTOR
AND THE PRINCIPAL DEPUTY NATIONAL CYBER DIRECTOR

FROM: Jen Berlin, Assistant National Cyber Director Stakeholder Engagement
Caitlin Clark, Assistant National Cyber Director Planning
Nick Leiserson, Assistant National Cyber Director Cyber Policy
Michael Morris, Assistant National Cyber Director Public Affairs
Jonathan Ring, Director, National Cybersecurity

SUBJECT: Hackers at The White House (HATWH) Concept

(b) (5)

(b) (5)



December 20, 2022

**OFFICE OF THE NATIONAL CYBER DIRECTOR
EXECUTIVE SECRETARY**

Tracking

NUMBER: 121922-002
VERSION: v (1.2)
DATE: 20 Dec 2022

Coordination and Approval

PREPARED BY: Jen Berlin, Assistant National Cyber Director for Stakeholder Engagement
Caitlin Clark, Assistant National Cyber Director Planning
Nick Leiserson, Assistant National Cyber Director Cyber Policy
Michael Morris, Assistant National Cyber Director Public Affairs
Jonathan Ring, Director, National Cybersecurity

CLEARED BY: Caroline Chang, Senior Advisor, ExecSec
Joe Scheidler, Special Advisor, ExecSec

Documents

ATTACHMENTS: N/A

BRIEFING MEMORANDUM

December 20, 2022

MEMORANDUM FOR THE NATIONAL CYBER DIRECTOR AND PRINCIPAL
DEPUTY NATIONAL CYBER DIRECTOR

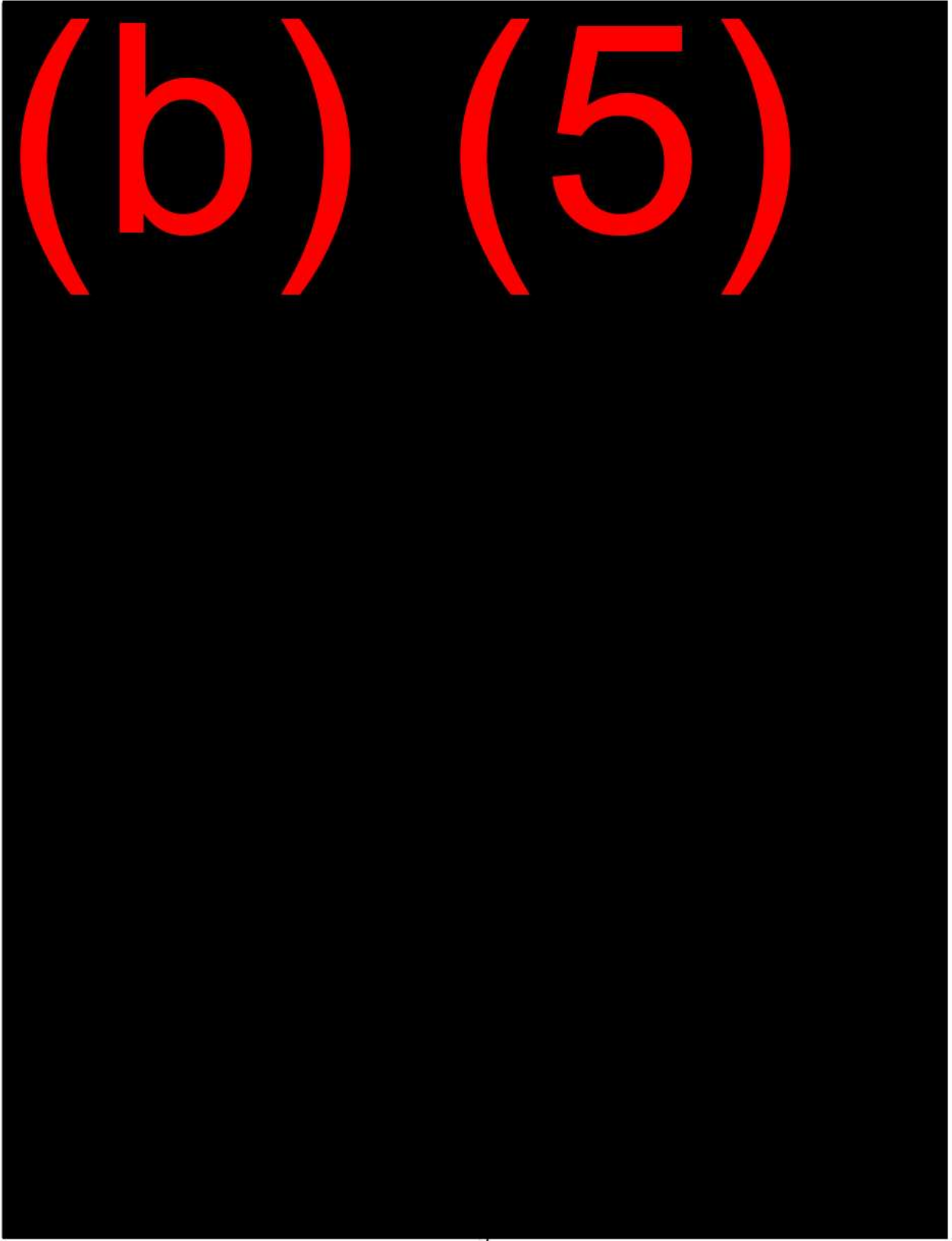
FROM: Philip Stupak, Director, Federal Cybersecurity

THROUGH: Camille Stewart Gloster, Deputy National Cyber Director, Technology & Ecosystem

SUBJECT: Africa Leaders' Summit Readout – Cybersecurity Meeting

(b) (5)

(b) (5)



Summary



**DRAFT//PRE-DECISIONAL
UNCLASSIFIED//FOR OFFICIAL USE ONLY**

December 20, 2022

**OFFICE OF THE NATIONAL CYBER DIRECTOR
EXECUTIVE SECRETARY**

Tracking

NUMBER: N/A
VERSION: v(1.2)
DATE: 15 December 2022

Coordination and Approval

PREPARED BY: Philip Stupak, (b) (6), (b) (6)
CLEARED BY: Camille Stewart Gloster, DNCD Technology and Ecosystem
Caroline Chang, Senior Advisor, ExecSec
Joe Scheidler, Special Advisor, ExecSec

Documents

ATTACHMENTS: Attendees

**DRAFT//PRE-DECISIONAL
UNCLASSIFIED//FOR OFFICIAL USE ONLY**

ATTACHMENT A: Attendees

International Government

- Michael Folane, Program Lead, PAYCR, Burkina Faso
- Wend-Panga Herman Ouedraogo, Technical Director, PAYCR, Burkina Faso
- Sekou Ouedraogo, Deputy Director of Intelligence, Burkina Faso
- Josue Toe, Administrative and Financial Head of Intelligence, Burkina Faso
- Mahamady Belem, Public Debt Director, Burkina Faso
- Colonel Pierre Ouedraogo, Head of Cybersecurity Center of Excellence, Burkina Faso
- Marc Andre Loko, CEO of ASIN, Benin
- Mahafous Osseni, Deputy Director, Port of Cotonou, Benin
- Ouanilo Medegan, Director of Security, Benin
- Henri Eyebe Ayissi, Minister of Domains, Cadaster and Land Affairs, Cameroon
- Lejeune Mbella, Minister of Foreign Affairs, Cameroon
- Alamine Ousmane Mey, Minister of Finance, Cameroon
- Mbarga Antagana, Minister of Commerce, Cameroon
- Sassou Nguesso, Minister of International Cooperation, Republic of the Congo
- Ibrahima Guimba, Head of Cybersecurity Agency, Niger
- Ahmat Jidoud, Minister of Finance, Niger

U.S. Government

- Camille Stewart Gloster, DNCD Technology & Ecosystem Security, ONCD, EOP
- Phil Stupak, Director of Federal Cybersecurity, ONCD, EOP
- Anne-Marie Mills, Senior Policy Advisor, CDP, Department of State
- Vanna Lavery, Cybersecurity & Digital Policy Office, CDP, Department of State
- Maurice Kent, Digital APEX Program Lead, USAID, Department of State
- Danica Starks, Head of Multilateral Development Bank Group, Department of Commerce
- Amy Mahn, International Policy Specialist, NIST, Department of Commerce
- Andrew Rollo, Vice President, China and Transformational Exports, Export-Import Bank

Industry

- Dr. Thierry Wandji, President and CEO, Cybastion
- Leila Ndiaye, SVP for Business Strategy & Government Affairs, Cybastion
- Andre Biyong, SVP of Operations, Cybastion
- Emana Shunnom, Senior Manager of Policy, Cybastion
- Alex Botting, Senior Director, Venable
- Tanvi Chopra, Cybersecurity Analyst, Venable
- Ari Schwartz, Coordinator, Cybersecurity Coalition

DRAFT//PRE-DECISIONAL
UNCLASSIFIED//FOR OFFICIAL USE ONLY

- Idrissa Nassa, Chairman, Coris Bank
- Stephane Tapsoba, Deputy Director for Burkina, Coris Bank

**UNCLASSIFIED//FOR OFFICIAL USE ONLY
DISCUSSION DRAFT//PRE-DECISIONAL//DELIBERATIVE**

December 15, 2022

**DECISION MEMORANDUM FOR THE NATIONAL CYBER DIRECTOR AND
PRINCIPAL DEPUTY NATIONAL CYBER DIRECTOR**

FROM: Harry Krejsa, ANCD Strategy and Research
Hannah Suh, Special Advisor

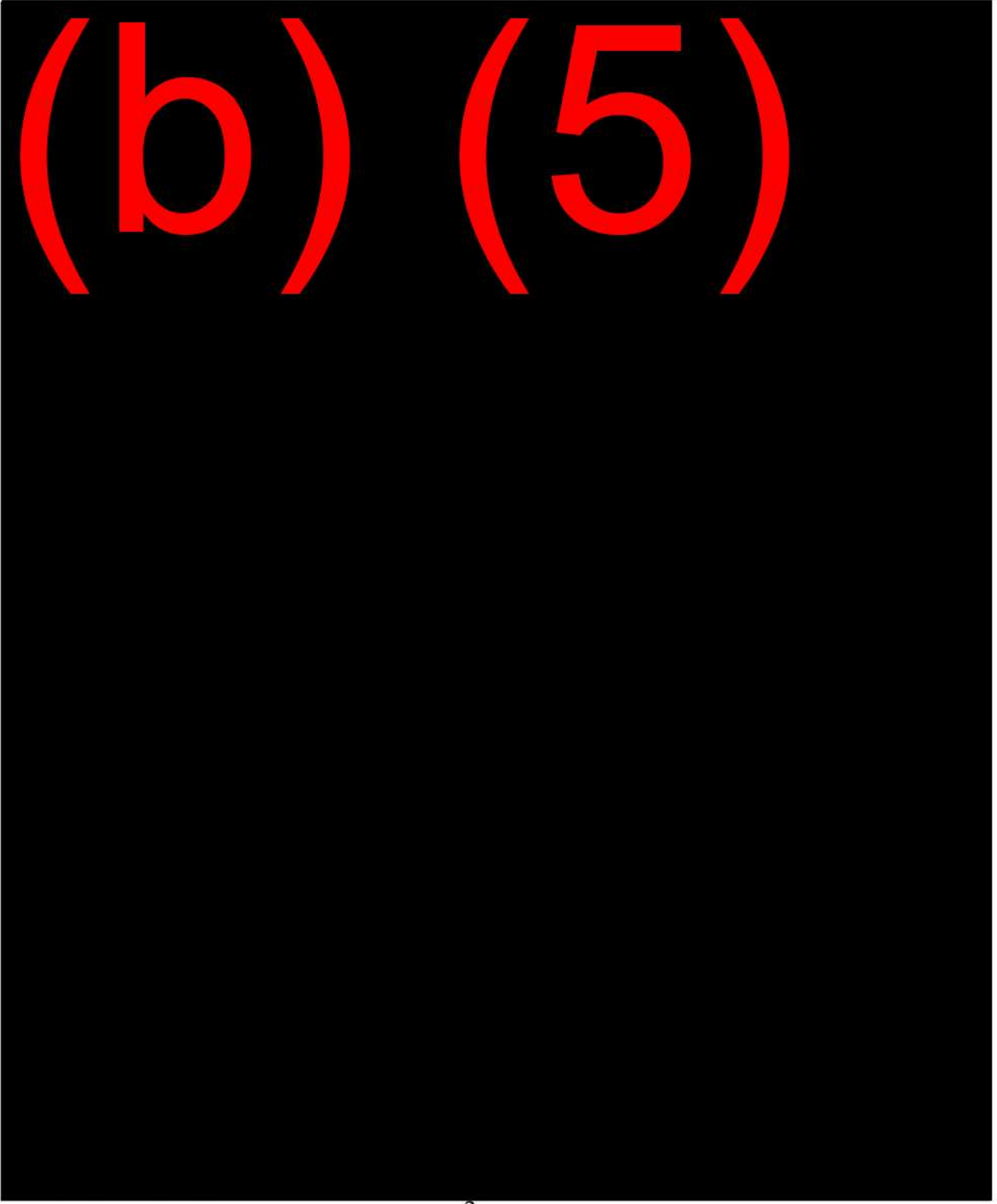
THROUGH: Michael Hochman, Chief of Staff

SUBJECT: ONCD International Engagements

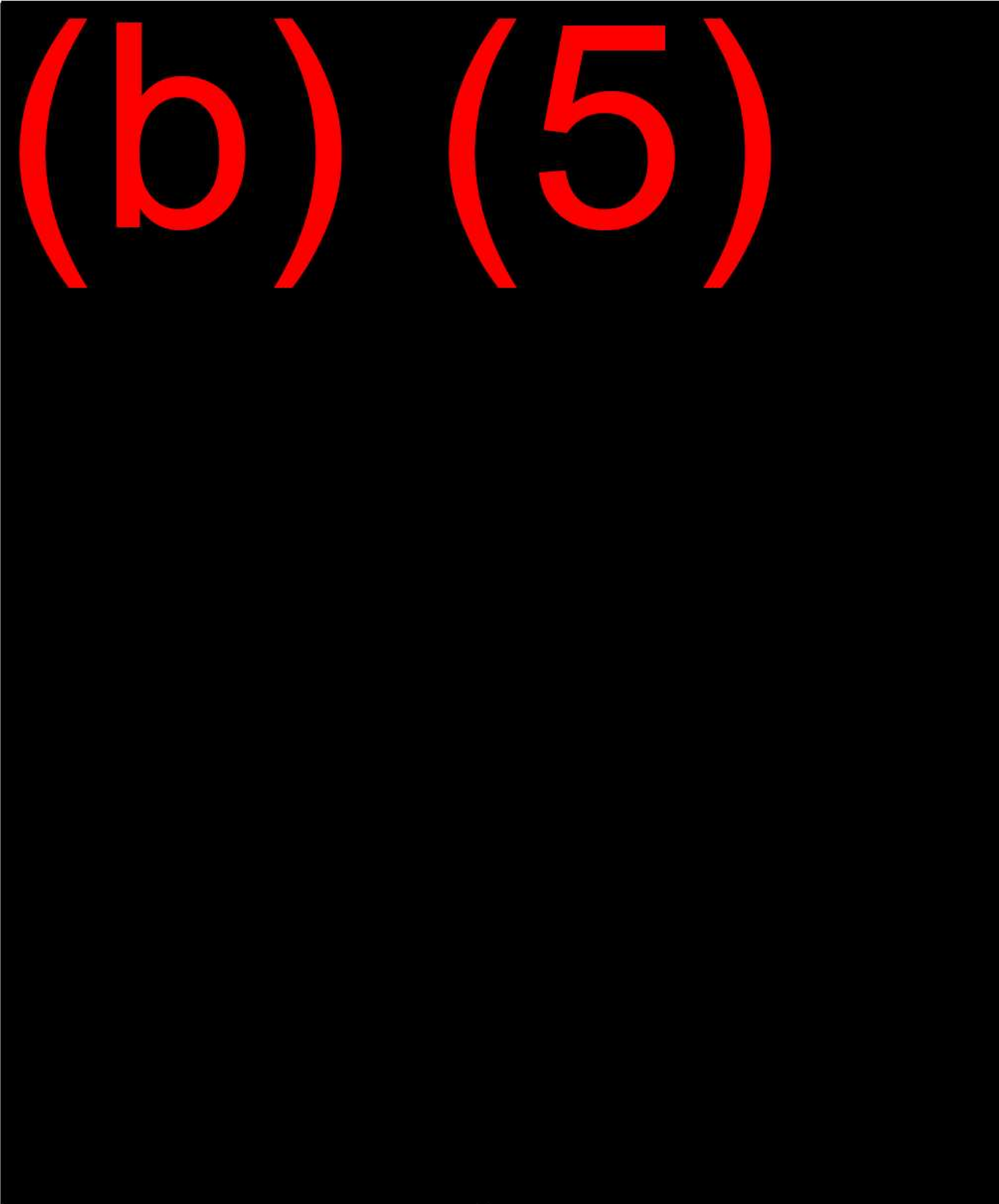
(b) (5)

**UNCLASSIFIED//FOR OFFICIAL USE ONLY
DISCUSSION DRAFT//PRE-DECISIONAL//DELIBERATIVE**

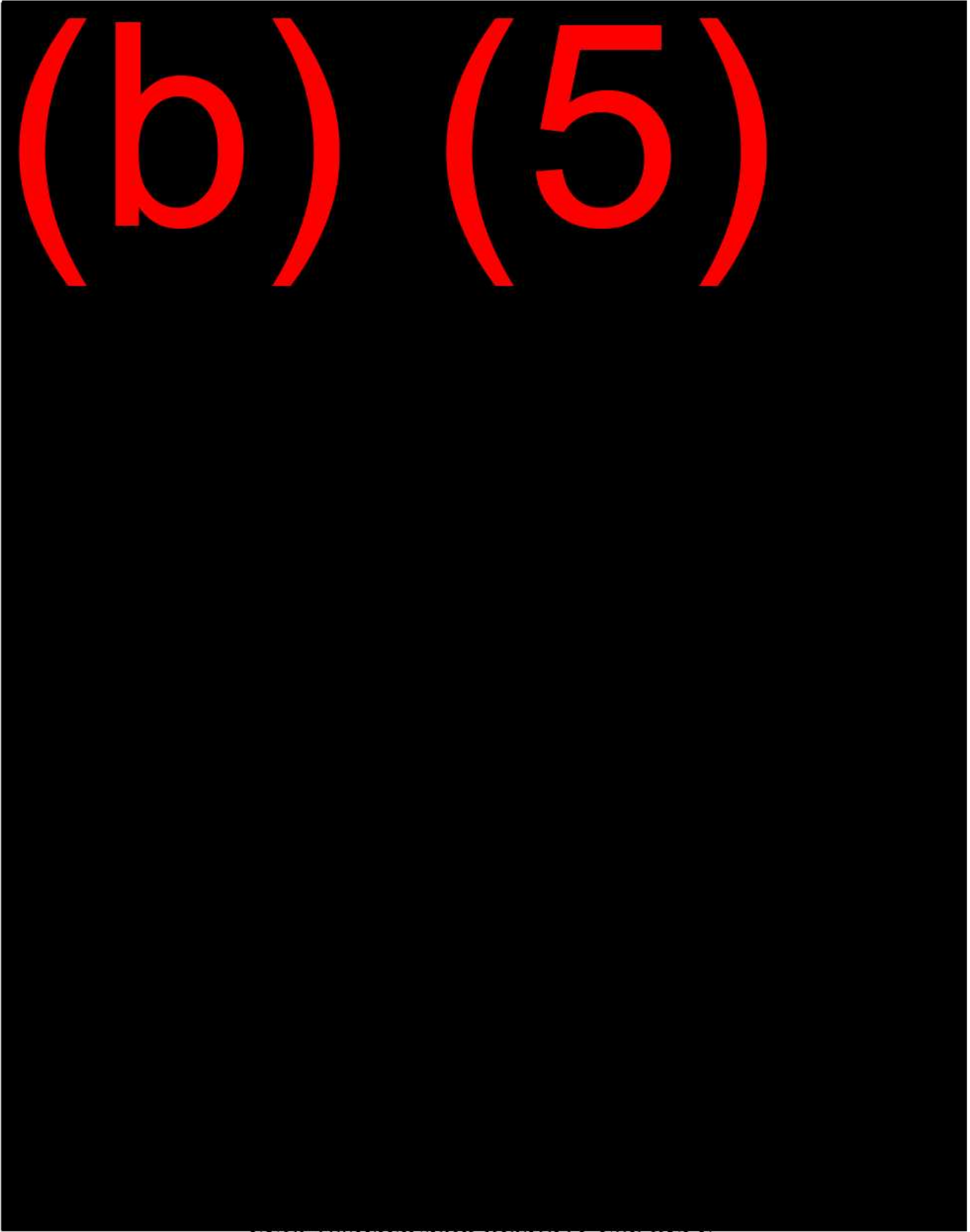
(b) (5)



(b) (5)

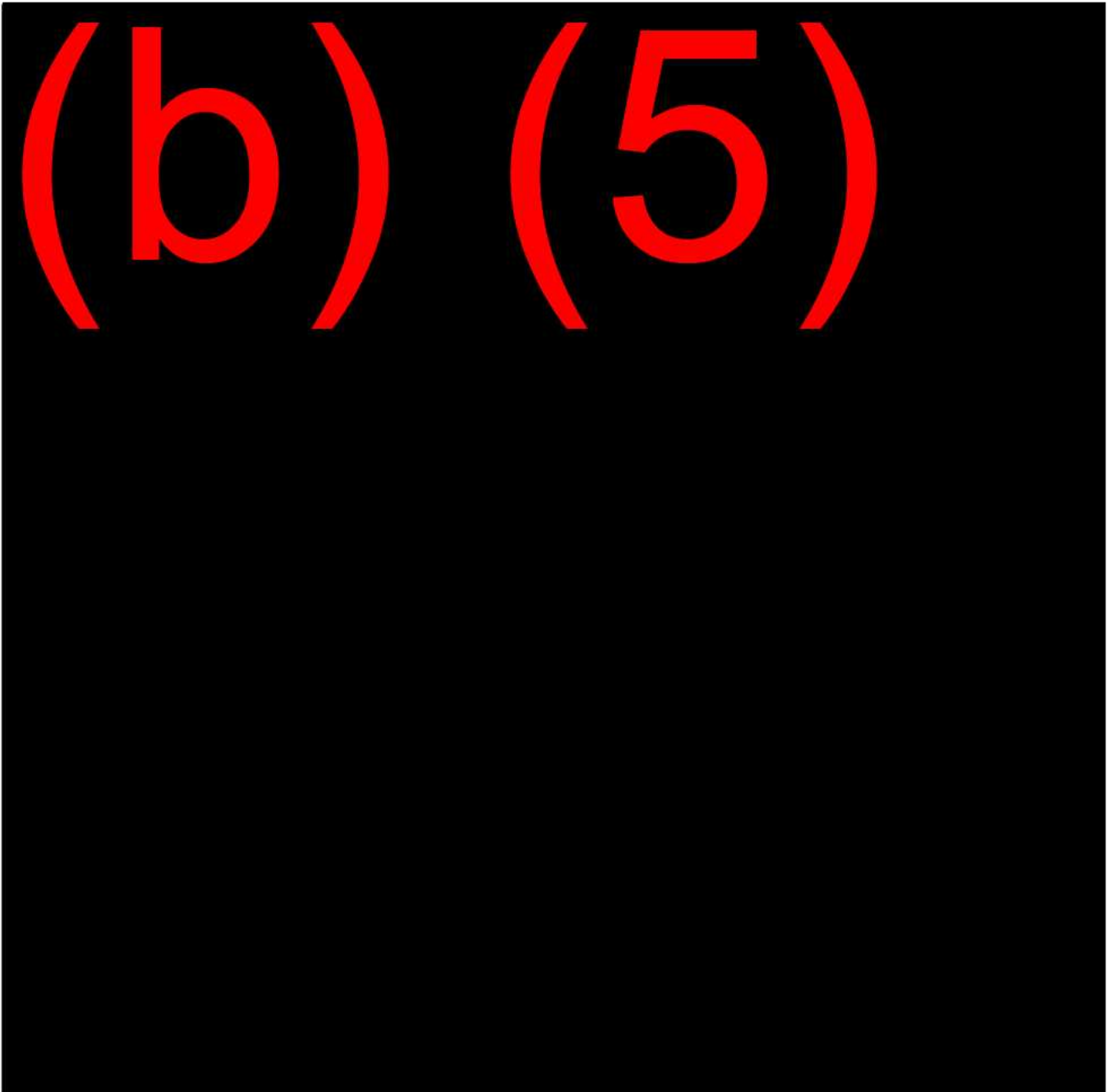


(b) (5)



(b) (5)

(b) (5)





December 15, 2022

OFFICE OF THE NATIONAL CYBER DIRECTOR DECISION

Approval and Coordination

1. **Scope and Impact.** ONCD and the interagency
2. **Coordinated and Approved.** This proposal was developed with all line divisions and has received clearance from the Deputies.

This decision memo was cleared by:

Caroline Chang, Senior Advisor, ExecSec
Michael Hochman, Chief of Staff

3. **Consulted.** N/A

Decision

Approve: _____	Approve as Amended: _____
Reject: _____	Discuss: _____
_____ JOHN C. INGLIS National Cyber Director Office of the National Cyber Director Executive Office of the President	_____ DATE

UNCLASSIFIED//FOR OFFICIAL USE ONLY
DISCUSSION DRAFT//PRE-DECISIONAL//DELIBERATIVE

Attachment A: Selections of Relevant Statutory Authorities

6 USC 1500 (National Cyber Director Act)

...

(c) Duties of the National Cyber Director

(1) In general

Subject to the authority, direction, and control of the President, the Director shall-

(A) serve as the principal advisor to the President on cybersecurity policy and strategy relating to the coordination of-

- (i) information security and data protection;
- (ii) programs and policies intended to improve the cybersecurity posture of the United States;
- (iii) efforts to understand and deter malicious cyber activity;
- (iv) efforts to increase the security of information and communications technology and services and to promote national supply chain risk management and vendor security;

(v) diplomatic and other efforts to develop norms and international consensus around responsible state behavior in cyberspace;

- (vi) awareness and adoption of emerging technology that may enhance, augment, or degrade the cybersecurity posture of the United States; and
- (vii) such other cybersecurity matters as the President considers appropriate;...

(2) Delegation of authority

(A) The Director may-

- (i) serve as the senior representative to any organization that the President may establish for the purpose of providing the President advice on cybersecurity;
- (ii) subject to subparagraph (B), be included as a participant in preparations for and, when appropriate, the execution of domestic and international summits and other international meetings at which cybersecurity is a major topic;**
- (iii) delegate any of the Director's functions, powers, and duties to such officers and employees of the Office as the Director considers appropriate; and
- (iv) authorize such successive re-delegations of such functions, powers, and duties to such officers and employees of the Office as the Director considers appropriate.

(B) In acting under subparagraph (A) (ii) in the case of a summit or a meeting with an international partner, the Director shall act in coordination with the Secretary of State...

FY23 NDAA Section 9502 (Cyber Diplomacy Act)

(a) In General.--Section 1 of the State Department Basic Authorities Act of 1956 (22 U.S.C. 2651a), is amended--

(1) by redesignating subsections (i) and (j) as subsection (j) and (k), respectively;

(2) by redesignating subsection (h) (as added by section 361(a)(1) of division FF of the Consolidated Appropriations Act, 2021 (Public Law 116-260)) as subsection (l); and

(3) by inserting after subsection (h) the following:

“(i) Bureau of Cyberspace and Digital Policy.--

“(1) In general.--There is established, within the Department of State, the Bureau of Cyberspace and Digital Policy (referred to in this subsection as the ‘Bureau’). The head of the Bureau shall have the rank and status of ambassador and shall be appointed by the President, by and with the advice and consent of the Senate.

UNCLASSIFIED//FOR OFFICIAL USE ONLY
DISCUSSION DRAFT//PRE-DECISIONAL//DELIBERATIVE

``(2) Duties.--

``(A) In general.--The head of the Bureau shall perform such duties and exercise such powers as the Secretary of State shall prescribe, including implementing the diplomatic and foreign policy aspects of the policy described in section 9501(a) of the Department of State Authorization Act of 2022.

``(B) Duties described.--The principal duties and responsibilities of the head of the Bureau shall, in furtherance of the diplomatic and foreign policy mission of the Department of State, be--

``(i) to serve as the principal cyberspace policy official within the senior management of the Department of State and as the advisor to the Secretary of State for cyberspace and digital issues;

``(ii) to lead, coordinate, and execute, in coordination with other relevant bureaus and offices, the Department of State's diplomatic cyberspace, and cybersecurity efforts (including efforts related to data privacy, data flows, internet governance, information and communications technology standards, and other issues that the Secretary has assigned to the Bureau);

``(iii) to coordinate with relevant Federal agencies and the Office of the National Cyber Director to ensure the diplomatic and foreign policy aspects of the cyber strategy in section 9501 of the Department of State Authorization Act of 2022 and any other subsequent strategy are implemented in a manner that is fully integrated with the broader strategy;

``(iv) to promote an open, interoperable, reliable, and secure information and communications technology infrastructure globally;

``(v) to represent the Secretary of State in interagency efforts to develop and advance Federal Government cyber priorities and activities, including efforts to develop credible national capabilities, strategies, and policies to deter and counter cyber adversaries, and carry out the purposes of title V of the Department of State Authorization Act of 2022;

``(vi) to engage civil society, the private sector, academia, and other public and private entities on relevant international cyberspace and international information and communications technology issues;

``(vii) to support United States Government efforts to uphold and further develop global deterrence frameworks for malicious cyber activity;

``(viii) to advise the Secretary of State and coordinate with foreign governments regarding responses to national security-level cyber incidents, including coordination on diplomatic response efforts to support allies and partners threatened by malicious cyber activity, in conjunction with members of the North Atlantic Treaty Organization and like-minded countries;

``(ix) to promote the building of foreign capacity relating to cyberspace policy priorities;

``(x) to promote an open, interoperable, reliable, and secure information and communications technology infrastructure globally and an open, interoperable, secure, and reliable internet governed by the multi-stakeholder model;

``(xi) to promote an international environment for technology investments and the internet that benefits

UNCLASSIFIED//FOR OFFICIAL USE ONLY
DISCUSSION DRAFT//PRE-DECISIONAL//DELIBERATIVE

United States economic and national security interests;
``(xii) to promote cross-border flow of data and
combat international initiatives seeking to impose
unreasonable requirements on United States businesses;
``(xiii) to promote international policies to
protect the integrity of United States and international
telecommunications infrastructure from foreign-based
threats, including cyber-enabled threats;
``(xiv) to lead engagement, in coordination with
relevant executive branch agencies, with foreign
governments on relevant international cyberspace,
cybersecurity, cybercrime, and digital economy issues
described in title V of the Department of State
Authorization Act of 2022;
``(xv) to promote international policies, in
coordination with the Department of Commerce, to secure
radio frequency spectrum in the best interests of the
United States;
``(xvi) to promote and protect the exercise of human
rights, including freedom of speech and religion,
through the internet;
``(xvii) to build capacity of United States
diplomatic officials to engage on cyberspace issues;
``(xviii) to encourage the development and adoption
by foreign countries of internationally recognized
standards, policies, and best practices;
``(xix) to support efforts by the Global Engagement
Center to counter cyber-enabled information operations
against the United States or its allies and partners;
and
``(xx) to conduct such other matters as the
Secretary of State may assign...

``(6) Coordination.--In implementing the duties prescribed under
paragraph (2), the head of the Bureau shall coordinate with the heads of
other Federal agencies, including the Department of Commerce, the
Department of Homeland Security, and other Federal agencies that the
National Cyber Director deems appropriate...

[Briefer's note on FY23 NDAA – The language referenced above passed the House on December 8, 2022, as part of the final NDAA negotiated between the House and Senate. The Senate is expected to take it up on or before December 16, 2022, after which it will go to the President for his signature. ONCD staff have very high confidence that this language will become law before the end of the calendar year.]

RE: FY '23 Omnibus Cyber Tracker

From: "Arnold, Alison B. EOP/OMB" (b) (6) >
To: "Phaup, Elliott R. EOP/NCD" (b) (6), "Herckis, Mitch D. EOP/OMB" <(b) (6)>, "Polk, Nick J. EOP/OMB" <(b) (6)>, "Lam, Kristine V. EOP/OMB" <(b) (6)>, "Jang, Yejin EOP/OMB" <(b) (6)>, "Nsor, Janice M. EOP/OMB" <(b) (6)>, "Mill, Eric R. EOP/OMB" <(b) (6)>
Cc: ONCD Legislative Affairs <(b) (6)>, "Barr, Lisa N. EOP/NCD" (b) (6), "Stupak, Philip M. EOP/NCD" <(b) (6)>, "Gibson, Carolyn T. EOP/OMB" <(b) (6)>
Date: Tue, 10 Jan 2023 09:40:15 -0500
Attachments: External Tracker - 117th - FY 23 Omnibus.pdf (1.52 MB)

Thanks, Elliott. Very helpful to cross reference with our quick list!

From: Phaup, Elliott R. EOP/NCD (b) (6) >
Sent: Monday, January 9, 2023 4:42 PM
To: Herckis, Mitch D. EOP/OMB <(b) (6)>; Arnold, Alison B. EOP/OMB <(b) (6)>; Polk, Nick J. EOP/OMB <(b) (6)>; Lam, Kristine V. EOP/OMB <(b) (6)>; Jang, Yejin EOP/OMB <(b) (6)>; Nsor, Janice M. EOP/OMB (b) (6); Mill, Eric R. EOP/OMB (b) (6) >
Cc: ONCD Legislative Affairs <(b) (6)>; Barr, Lisa N. EOP/NCD <(b) (6)>; Stupak, Philip M. EOP/NCD <(b) (6)>
Subject: RE: FY '23 Omnibus Cyber Tracker

Classic. Attaching the tracker this time. ☺

Best,

ERP

From: Phaup, Elliott R. EOP/NCD
Sent: Monday, January 9, 2023 4:40 PM
To: Herckis, Mitch D. EOP/OMB <(b) (6)>; Arnold, Alison B. EOP/OMB <(b) (6)>; Polk, Nick J. EOP/OMB <(b) (6)>; Lam, Kristine V. EOP/OMB (b) (6); Jang, Yejin EOP/OMB <(b) (6)>; Nsor, Janice M. EOP/OMB <(b) (6)>; Mill, Eric R. EOP/OMB <(b) (6)>
Cc: ONCD Legislative Affairs <(b) (6)>; Barr, Lisa N. EOP/NCD <(b) (6)>; Stupak, Philip M. EOP/NCD (b) (6) >
Subject: FY '23 Omnibus Cyber Tracker

OMB Colleagues:

Sharing a tracker we put together on cyber auths and a sampling of reporting requirements from the FY '23 omni. It doesn't include funding levels and isn't exhaustive, but we pulled out some interesting items, some of which you were likely already tracking. We've grouped it by category so you can get a sense of some of the themes Congress is interested in. Noteworthy trends identified include: Cloud Security; Critical Infrastructure & Small Business; Cyber Workforce & Education; Federal Cybersecurity Coordination & Improvement.

We thought you might find this helpful, feel free to share with other OMB colleagues, as needed.

Best,

Elliott Phaup

Special Advisor for Legislative Affairs
Office of the National Cyber Director
Executive Office of the President

(b) (6) (U)

(b) (6) (JWICS)

Mobile: (b) (6)



FY '23 Omnibus Cyber Authorities & Reports

*Unless otherwise stated, the JES for the FY 23 Omnibus (P.L. 117-328) also incorporates reporting requirements from House Appropriations Committee Reports. This tracker provides a large sampling of cyber reports and is not an exhaustive list.

(b) (5)



FY '23 Omnibus Cyber Authorities & Reports

*Unless otherwise stated, the JES for the FY 23 Omnibus (P.L. 117-328) also incorporates reporting requirements from House Appropriations Committee Reports. This tracker provides a large sampling of cyber reports and is not an exhaustive list.

(b) (5)



FY '23 Omnibus Cyber Authorities & Reports

*Unless otherwise stated, the JES for the FY 23 Omnibus (P.L. 117-328) also incorporates reporting requirements from House Appropriations Committee Reports. This tracker provides a large sampling of cyber reports and is not an exhaustive list.

(b) (5)



FY '23 Omnibus Cyber Authorities & Reports

*Unless otherwise stated, the JES for the FY 23 Omnibus (P.L. 117-328) also incorporates reporting requirements from House Appropriations Committee Reports. This tracker provides a large sampling of cyber reports and is not an exhaustive list.

(b) (5)



FY '23 Omnibus Cyber Authorities & Reports

*Unless otherwise stated, the JES for the FY 23 Omnibus (P.L. 117-328) also incorporates reporting requirements from House Appropriations Committee Reports. This tracker provides a large sampling of cyber reports and is not an exhaustive list.

(b) (5)



FY '23 Omnibus Cyber Authorities & Reports

*Unless otherwise stated, the JES for the FY 23 Omnibus (P.L. 117-328) also incorporates reporting requirements from House Appropriations Committee Reports. This tracker provides a large sampling of cyber reports and is not an exhaustive list.

(b) (6)



FY '23 Omnibus Cyber Authorities & Reports

*Unless otherwise stated, the JES for the FY 23 Omnibus (P.L. 117-328) also incorporates reporting requirements from House Appropriations Committee Reports. This tracker provides a large sampling of cyber reports and is not an exhaustive list.

(b) (5)



FY '23 Omnibus Cyber Authorities & Reports

*Unless otherwise stated, the JES for the FY 23 Omnibus (P.L. 117-328) also incorporates reporting requirements from House Appropriations Committee Reports. This tracker provides a large sampling of cyber reports and is not an exhaustive list.

(b) (5)

RE: TPs on Privacy and KYC EO

From: "Klein, Julie G. EOP/NCD" (b) (6)
To: "Halpert, James J. EOP/NCD" (b) (6), "Vina, Stephen R. EOP/NCD"
<(b) (6)>, "Laskai, Lorand C. EOP/NCD"
(b) (6) >, "Lee, Michaela A. EOP/NCD"
(b) (6) >, "Scott, Brian C. EOP/NCD" <(b) (6)>, "Cummings, John E. EOP/NCD" <(b) (6)>
Cc: "Phaup, Elliott R. EOP/NCD" (b) (6), "Tiao, Paul M. EOP/NCD" <(b) (6)>
Date: Mon, 06 Feb 2023 10:56:27 -0500

(b) (5)

Any edits to this privacy leg background info:

(b) (5)

From: Halpert, James J. EOP/NCD <(b) (6)>
Sent: Monday, February 6, 2023 9:28 AM
To: Vina, Stephen R. EOP/NCD <(b) (6)>; Laskai, Lorand C. EOP/NCD
(b) (6) >; Klein, Julie G. EOP/NCD <(b) (6)>; Lee, Michaela A. EOP/NCD (b) (6) >; Scott, Brian C. EOP/NCD
(b) (6) >; Cummings, John E. EOP/NCD <(b) (6)>
Cc: Phaup, Elliott R. EOP/NCD <(b) (6)>; Tiao, Paul M. EOP/NCD

<(b) (6)>

Subject: RE: TPs on Privacy and KYC EO

(b) (5)

If you could share the op-ed, I'd be happy to review. Thanks -- Jim

From: Vina, Stephen R. EOP/NCD <(b) (6)>

Sent: Monday, February 6, 2023 9:20 AM

To: Laskai, Lorand C. EOP/NCD <(b) (6)>; Klein, Julie G. EOP/NCD <(b) (6)>; Lee, Michaela A. EOP/NCD <(b) (6)>; Scott, Brian C. EOP/NCD <(b) (6)>; Cummings, John E. EOP/NCD <(b) (6)>

Cc: Phaup, Elliott R. EOP/NCD <(b) (6)>; Tiao, Paul M. EOP/NCD <(b) (6)>; Halpert, James J. EOP/NCD <(b) (6)>

Subject: RE: TPs on Privacy and KYC EO

+OGC

I do not believe ONCD has taken a position on a private right of action. (b) (5)

(b) (5)

From: Laskai, Lorand C. EOP/NCD <(b) (6)>

Sent: Monday, February 6, 2023 8:45 AM

To: Klein, Julie G. EOP/NCD <(b) (6)>; Lee, Michaela A. EOP/NCD <(b) (6)>; Scott, Brian C. EOP/NCD <(b) (6)>; Cummings, John E. EOP/NCD <(b) (6)>

Cc: Vina, Stephen R. EOP/NCD <(b) (6)>; Phaup, Elliott R. EOP/NCD <(b) (6)>

Subject: RE: TPs on Privacy and KYC EO

Nothing new. It's in the NCS + Biden's WSJ op-ed.

I'll leave the private right of action to Leg Affairs.

From: Klein, Julie G. EOP/NCD <(b) (6)>
Sent: Monday, February 6, 2023 8:36 AM
To: Laskai, Lorand C. EOP/NCD <(b) (6)>; Lee, Michaela A. EOP/NCD <(b) (6)>; Scott, Brian C. EOP/NCD <(b) (6)>; Cummings, John E. EOP/NCD <(b) (6)>
Cc: Vina, Stephen R. EOP/NCD <(b) (6)>; Phaup, Elliott R. EOP/NCD <(b) (6)>; Klein, Julie G. EOP/NCD <(b) (6)>
Subject: RE: TPs on Privacy and KYC EO

+ Leg

Lorand,

Has this privacy position been said out loud before or would Kemba be the first ONCD person opining on it?

Also, the two big sticking points in legislation are preemption and private right of action. Seems clear the federal government supports preemption. Does ONCD have a position on private right of action? (*likely a Leg Affairs question*)

From: Laskai, Lorand C. EOP/NCD <(b) (6)>
Sent: Friday, February 3, 2023 11:55 PM
To: Klein, Julie G. EOP/NCD <(b) (6)>; Lee, Michaela A. EOP/NCD <(b) (6)>; Scott, Brian C. EOP/NCD <(b) (6)>; Cummings, John E. EOP/NCD <(b) (6)>
Subject: RE: TPs on Privacy and KYC EO

Julie, apologies for the delay. Below are the TPs. If [@Scott, Brian C. EOP/NCD](#) has any thoughts on the TPs for KYC, he will follow up.

(b) (5)

(b) (5)

From: Klein, Julie G. EOP/NCD (b) (6) >
Sent: Thursday, February 2, 2023 10:20 AM
To: Laskai, Lorand C. EOP/NCD (b) (6) >; Lee, Michaela A. EOP/NCD <(b) (6)>; Scott, Brian C. EOP/NCD <(b) (6)>; Cummings, John E. EOP/NCD <(b) (6)>
Subject: RE: TPs on Privacy and KYC EO

Ok... I haven't actually compiled any of this yet... but will share when I do

Also, graph = paragraph/TPs (I'm apparently a 13 year old who abbreviates everything)

From: Laskai, Lorand C. EOP/NCD (b) (6) >
Sent: Thursday, February 2, 2023 10:08 AM
To: Klein, Julie G. EOP/NCD <(b) (6)>; Lee, Michaela A. EOP/NCD <(b) (6)>; Scott, Brian C. EOP/NCD (b) (6) >; Cummings, John E. EOP/NCD <(b) (6)>
Subject: RE: TPs on Privacy and KYC EO

I can take a look at the NCS TPs and make sure they're right.

[@Scott, Brian C. EOP/NCD](#) I'll pass some text on KYC by you.

From: Klein, Julie G. EOP/NCD <(b) (6)>
Sent: Thursday, February 2, 2023 10:06 AM
To: Laskai, Lorand C. EOP/NCD (b) (6) >; Lee, Michaela A. EOP/NCD <(b) (6)>; Scott, Brian C. EOP/NCD (b) (6) >; Cummings, John E. EOP/NCD (b) (6) >
Subject: RE: TPs on Privacy and KYC EO

THANK YOU!

Since we have a brain trust here, these are the topics I'm planning – let me know if I'm missing anything. (I have most of these TPs already)

(b) (5)

From: Laskai, Lorand C. EOP/NCD <(b) (6)>
Sent: Thursday, February 2, 2023 10:01 AM
To: Klein, Julie G. EOP/NCD <(b) (6)>; Lee, Michaela A. EOP/NCD <(b) (6)>; Scott, Brian C. EOP/NCD <(b) (6)>; Cummings, John E. EOP/NCD <(b) (6)>
Subject: RE: TPs on Privacy and KYC EO

Of course! I'm adding a few crucial folks who we'll coordinate w on the TPS.

[@Scott, Brian C. EOP/NCD](#) for KYC

[@Cummings, John E. EOP/NCD](#) for privacy

From: Klein, Julie G. EOP/NCD <(b) (6)>
Sent: Thursday, February 2, 2023 9:51 AM
To: Laskai, Lorand C. EOP/NCD <(b) (6)>; Lee, Michaela A. EOP/NCD <(b) (6)>
Subject: TPs on Privacy and KYC EO

Morning!

Next week Kemba is participating in a small salon dinner at the Chamber. Other participants are the CEO of CrowdStrike, Eric Goldstein, and someone (whose name is escaping me) from the FBI. (b) (5)

(b) (5)

(b) (5)

Would it be possible to get it to me by COB tomorrow?

Also, who should I ask for an ONCD position on encryption/going dark?

Thank you!!

jk

Re: TPs on Privacy and KYC EO

From: "Klein, Julie G. EOP/NCD" (b) (6) >
To: "Laskai, Lorand C. EOP/NCD" (b) (6) >
Cc: "Halpert, James J. EOP/NCD" <(b) (6)>, "Vina, Stephen R. EOP/NCD" <(b) (6)>, "Lee, Michaela A. EOP/NCD" <(b) (6)>, "Scott, Brian C. EOP/NCD" <(b) (6)>, "Cummings, John E. EOP/NCD" <(b) (6)>, "Phaup, Elliott R. EOP/NCD" (b) (6) >, "Tiao, Paul M. EOP/NCD" (b) (6) >
Date: Mon, 06 Feb 2023 11:00:30 -0500



Julie Klein
Principal Senior Advisor to the Principal Deputy National Cyber Director
Office of the National Cyber Director
Executive Office of the President
Mobile: (b) (6)

On Feb 6, 2023, at 10:58 AM, Laskai, Lorand C. EOP/NCD <(b) (6)> wrote:

No, it is not public. Kemba should not address it.

From: Klein, Julie G. EOP/NCD (b) (6) >
Sent: Monday, February 6, 2023 10:56 AM
To: Halpert, James J. EOP/NCD <(b) (6)>; Vina, Stephen R. EOP/NCD (b) (6); Laskai, Lorand C. EOP/NCD <(b) (6)>; Lee, Michaela A. EOP/NCD <(b) (6)>; Scott, Brian C. EOP/NCD <(b) (6)>; Cummings, John E. EOP/NCD <(b) (6)>
Cc: Phaup, Elliott R. EOP/NCD (b) (6) >; Tiao, Paul M. EOP/NCD (b) (6) >
Subject: RE: TPs on Privacy and KYC EO

(b) (5)

Any edits to this privacy leg background info:

(b) (5)

(b) (5)

From: Halpert, James J. EOP/NCD (b) (6) >
Sent: Monday, February 6, 2023 9:28 AM
To: Vina, Stephen R. EOP/NCD (b) (6) >; Laskai, Lorand C. EOP/NCD (b) (6) >; Klein, Julie G. EOP/NCD (b) (6) >; Lee, Michaela A. EOP/NCD (b) (6) >; Scott, Brian C. EOP/NCD (b) (6) >; Cummings, John E. EOP/NCD (b) (6) >
Cc: Phaup, Elliott R. EOP/NCD (b) (6) >; Tiao, Paul M. EOP/NCD (b) (6) >
Subject: RE: TPs on Privacy and KYC EO

(b) (5)

If you could share the op-ed, I'd be happy to review. Thanks -- Jim

From: Vina, Stephen R. EOP/NCD (b) (6) >
Sent: Monday, February 6, 2023 9:20 AM
To: Laskai, Lorand C. EOP/NCD (b) (6) >; Klein, Julie G. EOP/NCD (b) (6) >; Lee, Michaela A. EOP/NCD (b) (6) >; Scott, Brian C. EOP/NCD (b) (6) >; Cummings, John E. EOP/NCD (b) (6) >
Cc: Phaup, Elliott R. EOP/NCD (b) (6) >; Tiao, Paul M. EOP/NCD (b) (6) >; Halpert, James J. EOP/NCD (b) (6) >
Subject: RE: TPs on Privacy and KYC EO

+OGC

I do not believe ONCD has taken a position on a private right of action. (b) (5)

(b) (5)

From: Laskai, Lorand C. EOP/NCD (b) (6) >
Sent: Monday, February 6, 2023 8:45 AM
To: Klein, Julie G. EOP/NCD (b) (6) >; Lee, Michaela A. EOP/NCD <(b) (6)>; Scott, Brian C. EOP/NCD <(b) (6)>; Cummings, John E. EOP/NCD <(b) (6)>
Cc: Vina, Stephen R. EOP/NCD (b) (6) >; Phaup, Elliott R. EOP/NCD (b) (6) >
Subject: RE: TPs on Privacy and KYC EO

Nothing new. It's in the NCS + Biden's WSJ op-ed.

I'll leave the private right of action to Leg Affairs.

From: Klein, Julie G. EOP/NCD <(b) (6)>
Sent: Monday, February 6, 2023 8:36 AM
To: Laskai, Lorand C. EOP/NCD (b) (6) >; Lee, Michaela A. EOP/NCD <(b) (6)>; Scott, Brian C. EOP/NCD <(b) (6)>; Cummings, John E. EOP/NCD <(b) (6)>
Cc: Vina, Stephen R. EOP/NCD (b) (6) >; Phaup, Elliott R. EOP/NCD (b) (6) >; Klein, Julie G. EOP/NCD <(b) (6)>
Subject: RE: TPs on Privacy and KYC EO

+ Leg

Lorand,

Has this privacy position been said out loud before or would Kemba be the first ONCD person opining on it?

Also, the two big sticking points in legislation are preemption and private right of action. Seems clear the federal government supports preemption. Does ONCD have a position on private right of action? (*likely a Leg Affairs question*)

From: Laskai, Lorand C. EOP/NCD <(b) (6)>
Sent: Friday, February 3, 2023 11:55 PM
To: Klein, Julie G. EOP/NCD <(b) (6)>; Lee, Michaela A. EOP/NCD

<(b) (6)>; Scott, Brian C. EOP/NCD (b) (6)>
Cummings, John E. EOP/NCD <(b) (6)>
Subject: RE: TPs on Privacy and KYC EO

Julie, apologies for the delay. Below are the TPs. If [@Scott, Brian C. EOP/NCD](#) has any thoughts on the TPs for KYC, he will follow up.

(b) (5)

(b) (5)

From: Klein, Julie G. EOP/NCD (b) (6)>
Sent: Thursday, February 2, 2023 10:20 AM
To: Laskai, Lorand C. EOP/NCD (b) (6)>; Lee, Michaela A. EOP/NCD (b) (6)>; Scott, Brian C. EOP/NCD (b) (6)>
Cummings, John E. EOP/NCD <(b) (6)>
Subject: RE: TPs on Privacy and KYC EO

Ok... I haven't actually compiled any of this yet... but will share when I do

Also, graph = paragraph/TPs (I'm apparently a 13 year old who abbreviates everything)

From: Laskai, Lorand C. EOP/NCD <(b) (6)>
Sent: Thursday, February 2, 2023 10:08 AM
To: Klein, Julie G. EOP/NCD <(b) (6)>; Lee, Michaela A. EOP/NCD <(b) (6)>; Scott, Brian C. EOP/NCD <(b) (6)>; Cummings, John E. EOP/NCD <(b) (6)>
Subject: RE: TPs on Privacy and KYC EO

I can take a look at the NCS TPs and make sure they're right.

[@Scott, Brian C. EOP/NCD](#) I'll pass some text on KYC by you.

From: Klein, Julie G. EOP/NCD <(b) (6)>
Sent: Thursday, February 2, 2023 10:06 AM
To: Laskai, Lorand C. EOP/NCD <(b) (6)>; Lee, Michaela A. EOP/NCD <(b) (6)>; Scott, Brian C. EOP/NCD <(b) (6)>; Cummings, John E. EOP/NCD <(b) (6)>
Subject: RE: TPs on Privacy and KYC EO

THANK YOU!

Since we have a brain trust here, these are the topics I'm planning – let me know if I'm missing anything. (I have most of these TPs already)

(b) (5)

From: Laskai, Lorand C. EOP/NCD <(b) (6)>
Sent: Thursday, February 2, 2023 10:01 AM
To: Klein, Julie G. EOP/NCD <(b) (6)>; Lee, Michaela A. EOP/NCD <(b) (6)>; Scott, Brian C. EOP/NCD <(b) (6)>

Cummings, John E. EOP/NCD <(b) (6)>
Subject: RE: TPs on Privacy and KYC EO

Of course! I'm adding a few crucial folks who we'll coordinate w on the TPS.

[@Scott, Brian C. EOP/NCD](#) for KYC
[@Cummings, John E. EOP/NCD](#) for privacy

From: Klein, Julie G. EOP/NCD (b) (6) >
Sent: Thursday, February 2, 2023 9:51 AM
To: Laskai, Lorand C. EOP/NCD (b) (6) >; Lee, Michaela A. EOP/NCD <(b) (6)>
Subject: TPs on Privacy and KYC EO

Morning!

Next week Kemba is participating in a small salon dinner at the Chamber. Other participants are the CEO of CrowdStrike, Eric Goldstein, and someone (whose name is escaping me) from the FBI. I'm working on the memo, which is largely just TPs so she prepped on our cyber priorities and anything else that might come up.

(b) (5)
[Redacted]
[Redacted] Would it be possible to get it to me by COB tomorrow?

Also, who should I ask for an ONCD position on encryption/going dark?

Thank you!!
jk

RE: TPs on Privacy and KYC EO

From: "Vina, Stephen R. EOP/NCD" <(b) (6)>
To: "Laskai, Lorand C. EOP/NCD" <(b) (6)>, "Klein, Julie G. EOP/NCD" <julie.g.klein@ncd.eop.gov>, "Lee, Michaela A. EOP/NCD" <(b) (6)>, "Scott, Brian C. EOP/NCD" <(b) (6)>, "Cummings, John E. EOP/NCD" <(b) (6)>
Cc: "Phaup, Elliott R. EOP/NCD" <(b) (6)>, "Tiao, Paul M. EOP/NCD" <(b) (6)>, "Halpert, James J. EOP/NCD" <(b) (6)>
Date: Mon, 06 Feb 2023 09:20:07 -0500

+OGC

(b) (5)

From: Laskai, Lorand C. EOP/NCD <(b) (6)>
Sent: Monday, February 6, 2023 8:45 AM
To: Klein, Julie G. EOP/NCD <(b) (6)>; Lee, Michaela A. EOP/NCD <(b) (6)>; Scott, Brian C. EOP/NCD <(b) (6)>; Cummings, John E. EOP/NCD <(b) (6)>
Cc: Vina, Stephen R. EOP/NCD <(b) (6)>; Phaup, Elliott R. EOP/NCD <(b) (6)>
Subject: RE: TPs on Privacy and KYC EO

Nothing new. It's in the NCS + Biden's WSJ op-ed.

I'll leave the private right of action to Leg Affairs.

From: Klein, Julie G. EOP/NCD <(b) (6)>
Sent: Monday, February 6, 2023 8:36 AM
To: Laskai, Lorand C. EOP/NCD <(b) (6)>; Lee, Michaela A. EOP/NCD <(b) (6)>; Scott, Brian C. EOP/NCD <(b) (6)>; Cummings, John E. EOP/NCD <(b) (6)>
Cc: Vina, Stephen R. EOP/NCD <(b) (6)>; Phaup, Elliott R. EOP/NCD <(b) (6)>; Klein, Julie G. EOP/NCD <(b) (6)>
Subject: RE: TPs on Privacy and KYC EO

+ Leg

Lorand,

Has this privacy position been said out loud before or would Kemba be the first ONCD person opining on it?

Also, the two big sticking points in legislation are preemption and private right of action. Seems clear the federal government supports preemption. Does ONCD have a position on private right of action? (*likely a Leg Affairs question*)

From: Laskai, Lorand C. EOP/NCD (b) (6) >
Sent: Friday, February 3, 2023 11:55 PM
To: Klein, Julie G. EOP/NCD (b) (6) >; Lee, Michaela A. EOP/NCD <(b) (6)>; Scott, Brian C. EOP/NCD (b) (6) >; Cummings, John E. EOP/NCD <(b) (6)>
Subject: RE: TPs on Privacy and KYC EO

Julie, apologies for the delay. Below are the TPs. If [@Scott, Brian C. EOP/NCD](#) has any thoughts on the TPs for KYC, he will follow up.

(b) (5)

(b) (5)

From: Klein, Julie G. EOP/NCD <(b) (6)>
Sent: Thursday, February 2, 2023 10:20 AM
To: Laskai, Lorand C. EOP/NCD <(b) (6)>; Lee, Michaela A. EOP/NCD <(b) (6)>; Scott, Brian C. EOP/NCD <(b) (6)>; Cummings, John E. EOP/NCD <(b) (6)>
Subject: RE: TPs on Privacy and KYC EO

Ok... I haven't actually compiled any of this yet... but will share when I do

Also, graph = paragraph/TPs (I'm apparently a 13 year old who abbreviates everything)

From: Laskai, Lorand C. EOP/NCD <(b) (6)>
Sent: Thursday, February 2, 2023 10:08 AM
To: Klein, Julie G. EOP/NCD <(b) (6)>; Lee, Michaela A. EOP/NCD <(b) (6)>; Scott, Brian C. EOP/NCD <(b) (6)>; Cummings, John E. EOP/NCD <(b) (6)>
Subject: RE: TPs on Privacy and KYC EO

I can take a look at the NCS TPs and make sure they're right.

[@Scott, Brian C. EOP/NCD](#) I'll pass some text on KYC by you.

From: Klein, Julie G. EOP/NCD <(b) (6)>
Sent: Thursday, February 2, 2023 10:06 AM
To: Laskai, Lorand C. EOP/NCD <(b) (6)>; Lee, Michaela A. EOP/NCD <(b) (6)>; Scott, Brian C. EOP/NCD <(b) (6)>; Cummings, John E. EOP/NCD <(b) (6)>
Subject: RE: TPs on Privacy and KYC EO

THANK YOU!

Since we have a brain trust here, these are the topics I'm planning – let me know if I'm missing anything. (I have most of these TPs already)

(b) (5)

(b) (5)

From: Laskai, Lorand C. EOP/NCD (b) (6) >
Sent: Thursday, February 2, 2023 10:01 AM
To: Klein, Julie G. EOP/NCD (b) (6) >; Lee, Michaela A. EOP/NCD <(b) (6)>; Scott, Brian C. EOP/NCD <(b) (6)>; Cummings, John E. EOP/NCD (b) (6) >
Subject: RE: TPs on Privacy and KYC EO

Of course! I'm adding a few crucial folks who we'll coordinate w on the TPS.

[@Scott, Brian C. EOP/NCD](#) for KYC

[@Cummings, John E. EOP/NCD](#) for privacy

From: Klein, Julie G. EOP/NCD (b) (6) >
Sent: Thursday, February 2, 2023 9:51 AM
To: Laskai, Lorand C. EOP/NCD (b) (6) >; Lee, Michaela A. EOP/NCD (b) (6) >
Subject: TPs on Privacy and KYC EO

Morning!

Next week Kemba is participating in a small salon dinner at the Chamber. Other participants are the CEO of CrowdStrike, Eric Goldstein, and someone (whose name is escaping me) from the FBI. I'm working on the memo, which is largely just TPs so she prepped on our cyber priorities and anything else that might come up.

(b) (5)

Also, who should I ask for an ONCD position on encryption/going dark?

Thank you!!

jk

Legislative Affairs Weekly (LAW) - 02/06/23

From: "Logan, Julianna I. EOP/NCD" (b) (6) >
To: DL NCD ALL (b) (6) >
Cc: ONCD Legislative Affairs <(b) (6)>
Bcc: "Clarke, Caitlin M. EOP/NCD" <(b) (6)>
Date: Mon, 06 Feb 2023 17:16:53 -0500
Attachments: LegAffairs_Weekly_02.06.23.pdf (276.78 kB)

Good Afternoon,

This week's Legislative Affairs Weekly (LAW) is attached & [linked](#) for your convenience. Intext hyperlinks can be accessed via the attachment or sharepoint.

Have a nice evening!

Julianna Logan

Special Advisor for Legislative Affairs
Office of the National Cyber Director
Executive Office of the President

(b) (6)

Mobile: (b) (6)



Legislative Affairs Weekly

6 February 2023

On Deck for ONCD

2/6	Meeting	Sen. Gary Peters (D-MI)	NCD Inglis; PDNCD Walden
-----	---------	-------------------------	--------------------------

Of Interest

2/8	Organizational Meeting	House Committee on Homeland Security (CHS)
2/8	Organizational Meeting	House Committee on Appropriations
2/9	Organizational Meeting	Senate Homeland Security & Governmental Affairs (HSGAC)

News of Note

- **Rep. Nancy Mace (R-SC-01) was appointed Chairwoman of the COA Subcommittee on Cybersecurity, Information Technology, and Government Innovation.** Upon her appointment, Rep. Mace stated “*Securing our nation's data, protecting our cyber infrastructure, and studying emerging technologies of the future like artificial intelligence, quantum computing, and blockchain integration is more important today than ever.*” (Mace, [Press Release](#), 02/01/2023). “Since coming to Congress in 2021, Rep. Mace has amassed a robust profile of cyber and IT legislative efforts, including work on the Quantum Computing Cybersecurity Preparedness Act.” (C. Burgan, [Meritalk](#); 2/3/23)
- **Rep. Gerry Connolly (D-VA-11) will serve as Ranking Member on COA’s Subcommittee on Cybersecurity, Information Technology, and Government Innovation.**
- Senator Roger Marshall (KS) joined HSGAC.
- New Members announced for ONCD oversight committees/subcommittees, see rosters below.

Legislation*

Under Suspension¹ in the House:

- [H.R. 302](#) - *Energy Cybersecurity University Leadership Act of 2023* | Rep. Ross, Deborah K. [D-NC] | Referred to House Science
 - Direct the Sec. of Energy to establish a program to provide financial assistance to graduate students and postdoctoral researchers pursuing certain courses relating to cybersecurity and energy infrastructure

Introduced:

- [S. 85](#) - *No TikTok on United States Devices Act* | Sen. Hawley (R-MO) | Referred to Committee on Banking, Housing, and Urban Affairs
 - Requires President to exercise all powers granted to prevent the commercial operation of TikTok in the U.S.
- [H.R. 503](#) - *No TikTok on United States Devices Act* | Rep. Buck, Ken (R-CO) | Referred to HFAC and HPSCI
 - Note: See Senate companion bill above.

¹ Under suspension, floor debate is limited, all floor amendments are prohibited, points of order against the bill are waived, and final passage requires a two-thirds majority vote.

*Not exhaustive

UNCLASSIFIED//FOR OFFICIAL USE ONLY//DELIBERATIVE//PRE-DECISIONAL

Committee Membership		
	Majority	Minority
Senate Committee on Homeland Security & Governmental Affairs (HSGAC)	Chairman Gary Peters (MI) Thomas R. Carper (DE) Margaret Hassan (NH) Kyrsten Sinema (AZ) Jacky Rosen (NV) Alex Padilla (CA) Jon Ossoff (GA) Richard Blumenthal (CT)	Ranking Member Rand Paul (KY) Ron Johnson (WI) James Lankford (OK) Mitt Romney (UT) Rick Scott (FL) Josh Hawley (MO) Roger Marshall (KS)
House Committee on Oversight & Accountability (COA)	Chairman James Comer (KY) Jim Jordan (OH) Mike Turner (OH) Paul Gosar (AZ) Virginia Foxx (NC) Glenn Grothman (WI) Gary Palmer (AL) Clay Higgins (LA) Andy Biggs (AZ) Nancy Mace (SC) Jake LaTurner (KS) Pat Fallon (TX) Byron Donalds (FL) Pete Sessions (TX) Kelly Armstrong (ND) Scott Perry (PA) William Timmons (SC) Tim Burchett (TN) Marjorie Taylor Greene (GA) Lisa McClain (MI) Lauren Boebert (CO) Russell Fry (SC) Anna Paulina Luna (FL) Chuck Edwards (NC) Nick Langworthy (NY) Eric Burlison (MO)	Ranking Member Jamie Raskin (MD) Eleanor Holmes Norton (DC) Stephen Lynch (MA) Gerald Connolly (VA) Raja Krishnamoorthi (IL) Ro Khanna (CA) Kweisi Mfume (MD) Alexandria Ocasio-Cortez (NY) Katie Porter (CA) Cori Bush (MO) Shontel M. Brown (OH) Jimmy Gomez (CA) Melanie Stansbury (NM) Robert Garcia (CA) Maxwell Frost (FL) Becca Balint (VT) Summer Lee (PA) Greg Casar (TX) Jasmine Crockett (TX) Dan Goldman (NY) Jared Moskowitz (FL)
House Committee on Homeland Security (CHS)	Chairman Mark E. Green, MD (R-TN) Michael McCaul (TX) Clay Higgins (LA) Michael Guest (MS) Dan Bishop (NC) Carlos Gimenez (FL) August Pfluger (TX) Andrew Garbarino (NY) Marjorie Taylor Greene (GA) Tony Gonzales (TX) Nick LaLota (NY) Mike Ezell (MS) Anthony D'Esposito (NY) Laurel Lee (FL) Morgan Luttrell (TX) Dale Strong (AL) Josh Brecheen (OK) Eli Crane (AZ)	Ranking Member Bennie Thompson (MS) Sheila Jackson Lee (TX) Donald M. Payne, Jr. (NJ) Eric Swalwell (CA) Lou Correa (CA) Troy Carter (LA) Shri Thanedar (MI) Seth Magaziner (RI) Glenn Ivey (MD) Dan Goldman (NY) Robert Garcia (CA) Delia Ramirez (IL) Rob Menendez (NJ) Yvette Clarke (NY) Dina Titus (NV)

*Not exhaustive

	Majority	Minority
House Committee on Appropriations - Financial Services and General Government Sub Committee (FSGG)	Steve Womack (AR) – Subcommittee Chair Mark Amodei (NV) Dave Joyce (OH) John Moolenaar (MI) Ashley Hinson (IA) Michael Cloud (TX) Jerry Carl (AL) Juan Ciscomani (AZ) Kay Granger (TX) – Ex Officio	Ranking Member Steny Hoyer (MD) Matt Cartwright (PA) Mark Pocan (WI) Sanford Bishop, Jr. (GA) Norma Torres (CA) Rosa DeLauro (CT) — Ex Officio
House Financial Services: Subcommittee on Digital Assets, Financial Technology and Inclusion	French Hill, (AR) Subcommittee Chair Frank D. Lucas (OK) Tom Emmer (MN) Warren Davidson (OH) John Rose (TN) Bryan Steil (WI) William Timmons (SC) Byron Donalds (FL) Mike Flood (NE) Erin Houchin (IN)	Ranking Member Stephen Lynch (MA) Bill Foster (IL) Josh Gottheimer (NJ) Ritchie Torres (NY) Brad Sherman (CA) Al Green (TX) Sean Casten (IL) Wiley Nickel (NC)

*Not exhaustive