From: Sendek, Sara (b) (6)
(b) (6)
Wales, Brandon (b) (6)
Hale, Geoffrey (b) (6)
(b) (6)
Kolasky, Robert (b) (6)
Early, Emily (b) (6)
To: (b) (6)
(b) (6)
Benacci, Kevin (b) (6)
(b) (6)
(b) (6)
Snell, Allison (b) (6)
(b) (6)
>;
Kroese, Daniel (b) (6)
Subject: RE: PSA for Approval
Date: 2020/12/23 14:44:01
Priority: Normal
Type: Note

Flagging the FBI was making some additional edits to the PSA which is why it's not out yet. Attached is the latest. These are all minor edits. We do not object.

From: Wales, Brandon (b) (6)
Sent: Tuesday, December 22, 2020 8:49 PM
To: Hale, Geoffrey (b) (6); Sendek, Sara (b) (6); Kolasky, Robert (b) (6); Early, Emily (b) (6); Benacci, Kevin (b) (6); Snell, Allison (b) (6); Kroese, Daniel (b) (6)
Subject: Re: PSA for Approval

No objection.

Brandon D. Wales
Cybersecurity and Infrastructure Secuity Agency (CISA)
Mobile: (b) (6)

From: Hale, Geoffrey (b) (6)
Sent: Tuesday, December 22, 2020 8:46:19 PM
To: Sendek, Sara (b) (6); Wales, Brandon (b) (6); Kolasky, Robert (b) (6); Early, Emily (b) (6); Benacci, Kevin

TLP: AMBER

Sender: CISA CurOps (b) (6) [redacted]

Recipient: CISA CurOps (b) (6) [redacted]
(b) (6) [redacted] >;
CISA Daily Ops (b) (6) [redacted]

Sent Date: 2020/12/28 07:50:07

Delivered Date: 2020/12/28 07:50:48

Message Flags: Unread

DIRECTOR'S WEEKLY OPERATIONS INFOGRAPHIC

December 28, 2020

CISA CENTRAL
202.282.9201

ALERT LEVELS

NTAS	None	Bulletin	Elevated	Imminent
NOC	Steady State	Awareness	Guarded	Concern	Urgent

OPERATION & SITUATION UPDATES

COVID-19

- For COVID-19 statistics, US Total cumulative cases are approximately 18.9 million with deaths near 331,000
- New cases in the last 7 days: 1,317,150
- New deaths in the last 7 days : 1,309
- Shipments of Pfizer and Moderna's FDA-authorized COVID-19 vaccine are arriving at sites across the US.
- Total Doses Distributed so far are approximately 9.5 million with Doses Administered over 1.9 million.

ENGAGEMENTS

- 28 DEC: (A)DAD Walsh will attend the ESCC: COVID-19 Coordination Call.

CONGRESSIONAL AFFAIRS

- No Scheduled Events

INTERNATIONAL AFFAIRS

- No Scheduled Events

	(A)DIR	(A)D/DIR	COS	(A)DAD ISD	(A)AD CSD	AD ECD	AD IOD	AD SED	AD NRMC
Today	NCR	NCR	NCR	NCR	NCR	NCR	NCR	NCR	NCR
Tomorrow	NCR	NCR	NCR	NCR	NCR	NCR	NCR	NCR	NCR

From: (b) (6)
(b) (6)
(b) (6)

To: Hale, Geoffrey (b) (6)
(b) (6)
(b) (6)
Snell, Allison (b) (6)
(b) (6)

Subject: Fwd: Warnings of Runoff related Violence In GA
Date: 2020/12/28 18:24:30
Priority: Normal
Type: Note

Geoff,

Are you able to join a briefing for Chairman Thompson at 1:00 tomorrow (Tuesday) regarding our work with GA? I know (b) (6) and (b) (6) are tracking down others from HQ to potentially brief as well. Let me know. The FAR referenced below from last week is attached.

From: (b) (6)
Sent: Monday, December 28, 2020 9:58 AM
To: (b) (6)
Cc: (b) (6)
(b) (6) Wieczorek, Erin (b) (6) ; LUJAN, MARIA; (b) (6)
Subject: Re: Warnings of Runoff related Violence In GA

(b) (6),

Please see the attached FAR which should be helpful to the Chairman. (b) (6) (copied) at DHS HQ is looking at availability for a briefing. What are some scheduling options for the Chairman?

(b) (6)

Get Outlook for iOS

From: (b) (6)
Sent: Saturday, December 26, 2020 9:07:14 AM
To: Wieczorek, Erin (b) (6)
Cc: (b) (6)
(b) (6)
Subject: Warnings of Runoff related Violence In GA

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Hi (b) (6) and (b) (6),

I hope you all had a good holiday. The Chairman has been reading about warnings of violence in GA related to the runoffs and asked us this morning for an unclassified briefing from DHS. Can you all help us with this request?

Thank you,
(b) (6)

Sender: (b) (6) (b) (6) (b) (6)

Recipient: Hale, Geoffrey (b) (7)(A)
Snell, Allison (b) (6)
(b) (6)

Sent Date: 2020/12/28 18:23:59

Delivered Date: 2020/12/28 18:24:30

FIELD ANALYSIS REPORT

Regional Analysis with National Perspective.

22 December 2020

(U//FOUO) Threat Environment Leading into US Senate Runoff Election in Georgia

(U//FOUO) Prepared by the Department of Homeland Security Intelligence Enterprise (DHS IE) Field Operations Division (FOD) - Southeast Region, Counterterrorism Mission Center (CTMC), Cyber Mission Center (CYMC), and the Georgia Bureau of Investigation – Georgia Information Sharing and Analysis Center (GBI-GISAC). Coordinated with the DHS Cybersecurity and Critical Infrastructure Security Agency (CISA) and the FBI Cyber Division, Major Cyber Crimes Intelligence Unit.

(U//FOUO) ***Scope:*** *This* Field Analysis Report (FAR) *examines details of physical threats, malicious cyber incidents, and foreign influence operations potentially impacting or indicative of potential threats to the US Senate runoff election in Georgia on 5 January 2021. This* FAR *only includes incidents potentially harmful to human life or disruptive to US election security and does not cover other election-related crimes or grievances.*

(U) Key Judgments

- (U//FOUO) **We judge that Georgia faces a potentially heightened physical threat environment over the course of its US Senate runoff election cycle, which may drive ideologically motivated violence or threats of violence similar to those seen nationwide during the 2020 presidential and state election season.**

- (U//FOUO) **We judge that incidents similar to those observed during the 2020 presidential election season—including unattributed suspicious scanning or probing of cyber networks, indirect impacts from ransomware and other cybercrime, or network disruptions not associated with malicious activity—likely could occur again during the runoff election, but their impact would be similarly minimal.** We do not have any indications that nation-state adversaries or other malicious cyber actors attempted to alter any technical aspects of Georgia election networks or systems during the November 2020 election or are attempting to disrupt or interfere with Georgia's election networks ahead of the US Senate runoff election.

- (U//FOUO) **We assess that foreign threat actors view the national significance of Georgia's US Senate runoff election as an opportunity to use social media and other influence tactics focused on the state.**

IA-48260-21

(U//FOUO) Potential for Heightened Physical Threat Environment Leading into Runoff Election

(U//FOUO) **We judge that Georgia faces a potentially heightened physical threat environment over the course of its US Senate runoff election cycle, which may drive ideologically motivated violence or threats of violence similar to those seen nationwide leading into the 2020 presidential and state election season.** We base this assessment on a review of national and local media coverage, relevant social media postings, state law enforcement officials detailing ideologically motivated violence or threats of violence, and DHS election violence assessments that have been disseminated over the previous six months.[a] Incidents of violence in or near the state capitol, courts, and other symbolic political institutions—similar to dozens of incidents observed nationwide—could also negatively impact elected officials or election workers in Georgia over the course of the election cycle. We further judge that violent extremists or other actors could quickly mobilize to violence or generate violent disruptions of otherwise lawful protests in response to a range of issues, including possible disputes over the results of the US presidential election.

(U) Georgia's US Senate Runoff Election

(U) Georgia is holding a runoff election for both of its US Senate seats on 5 January 2021. Under Georgia state law, the top two candidates for a seat must compete in a runoff when neither candidate receives the required majority (i.e., more than 50%) of the vote. States rarely have both US Senate seats open during the same election, and both seats being subject to simultaneous runoff elections is unusual. Georgia's runoff election will decide which party controls the US Senate and is expected to draw significant national attention, according to multiple US national media outlets.

- (U//FOUO) As of early December 2020, individuals involved in Georgia's audit and subsequent recount of votes for the US presidential election continue to report receiving death threats, according to US national and local media coverage and state law enforcement reporting. The Georgia Secretary of State (SOS) and election systems manager received precautionary protective security details while law enforcement officials investigated the credibility of threats made against him, according to an additional US news website. In a separate case, unknown individuals displayed a noose and threatened to hang a Georgia-based contract employee for "treason" in retaliation for working on the recount, according to a US national public news source.

- (U//LES) As recently as 21 November 2020, members of groups with opposing ideological views engaged in assaults and physical altercations in front of the Georgia State Capitol in Atlanta during otherwise peaceful demonstrations centered around grievances over the outcome of the US presidential election, according to information derived from a state fusion center. Police erected barricades between the groups to prevent further violence and eventually dispersed the crowds.

(U//FOUO) Limited Calls for Violence Nationwide Could Foreshadow Violent Rhetoric as Attention Shifts to Georgia

(U//FOUO) Nationwide, potentially violent incidents related to the election and its subsequently disputed results have been minimal, according to a DOJ official press release and a review of relevant social media postings. Nonetheless, limited and fragmentary cases of calls for violence across the country in reaction to the election's result indicate a potential for heightened violent rhetoric in Georgia should violent actors turn their attention to the state's US Senate race.

- *(U) An individual from New York faces federal charges after their 10 November 2020 arrest for allegedly posting multiple threats on social media to kill protestors, politicians, and law enforcement officers in retaliation for the outcome of the US presidential election, according to a DOJ press release.*
- *(U//FOUO) As of early December 2020, individuals in at least Texas and California posted unfulfilled threats to carry out violent attacks against political and ideological rivals in reaction to the election's results, according to relevant social media postings.*

[a] (U//FOUO) Please refer to the DHS I&A U//FOUO Intelligence In Focus titled, "Physical Threats to the 2020 Election Season", dated 17 August 2020, for additional details.

- (U//LES) In two separate July 2020 incidents, large groups of unidentified actors attacked federal and state law enforcement buildings in the Atlanta metro area as lawful protests were underway elsewhere in the city and state, according to a body of US national and local media reporting, relevant social media postings, and federal and state law enforcement information. On the night of 25 July 2020, approximately 100 people chanting "burn it down" smashed windows and ignited fireworks embedded with nails in an attempt to set fire to the US Immigration and Customs Enforcement (ICE) building in downtown Atlanta. On 5 July 2020, up to 100 people broke windows and used fireworks to light fires at the Georgia State Patrol headquarters, which is adjacent to the building that would later house the state's November 2020 election-night operations center, according to a separate US national media article.

(U//FOUO) Some Limited Network Disruptions Could Occur, but No Significant Impact to Election Systems Expected

(U//FOUO) **We judge that incidents similar to those observed during the 2020 presidential election season—including unattributed suspicious scanning or probing of cyber networks, indirect impacts from ransomware and other cybercrime, or network disruptions not associated with malicious activity—likely could occur again during the runoff election.** We do not have any indications that nation-state adversaries or other malicious cyber threat actors attempted to alter any technical aspects of Georgia election networks or systems during the November 2020 election or are attempting to disrupt or interfere with Georgia's election network ahead of the US Senate runoff election. We base this judgment on a review of DHS field reporting derived from state and local officials, a local US newspaper report, and incidents reported to state officials during the 2020 election season. We further assess that such activity could disrupt election infrastructure or cause delays at polling places. During the 2020 US presidential election season, we observed several incidents that caused minimal or indirect impacts to election systems, according to the same review.

- (U//FOUO) In mid-October 2020, unknown malicious cyber threat actors successfully infected a Georgia county network with a DopplePaymer ransomware variant, according to a DHS I&A field report derived from a county employee with access to cyber network defense information. Although the ransomware did not impact the state election system, it rendered a local copy of voter signature files saved on a county server and a geographic information system map of county polling locations temporarily inaccessible for several days during early voting, according to the same DHS I&A field report and a local US newspaper website.

- (U//FOUO) During late June 2020, unidentified malicious cyber threat actors, using a possible foreign-based IP address, unsuccessfully attempted to connect to a Georgia state network associated with election systems, according to a DHS I&A field report derived from a state official with access to cyber information. The IP addresses accessed an open Virtual Private Network port, but the gateway firewall blocked any further connections, according to the same report.

- (U//FOUO) On the day of Georgia's primary election, 9 June 2020, unidentified malicious cyber threat actors sent at least nine identical bitcoin extortion e-mails to the official e-mail address of a Georgia county election official, according to a DHS I&A field report derived from a county information technology official. The victim did not pay and successfully deleted and removed the e-mails without any compromise to the county network, according to the same report.

(U) US Presidential Election Day Network Issues Not Malicious, Caused No Serious Disruptions

(U//FOUO) On 3 November 2020, at least six Georgia counties experienced intermittent issues with equipment at some polling locations, according to a review of Election Day incidents reported to state, local, and federal officials. None of the incidents were malicious nor significantly impacted election operations; some polling places briefly switched to paper ballots—as is standard practice—while remediating encountered issues, according to the same review.

(U//FOUO) Foreign Threat Actors View Georgia's US Senate Runoff as Opportunity to Amplify Divisive and Misleading Information

(U//FOUO) We assess that foreign threat actors view the national significance of Georgia's US Senate runoff election as an opportunity to use social media and other influence tactics focused on the state, judging from a review of foreign state-run media coverage of the runoff election. We further assess that foreign influence actors could attempt to leverage any real or perceived physical or cyber incident to sow discord and create distrust in the election process in advance of the runoff election, based on our observations of previous influence operations targeting the US election. Russian and Iranian influence actors have previously targeted Georgia during election seasons, as evidenced in Russian and Iranian state-run media campaigns. Since 3 November 2020, Iranian and Russian state media outlets have amplified misleading content regarding Georgia's election results, efforts to recount votes, and civil unrest in Georgia, according to multiple foreign state-run media articles. Iranian and Russian state media outlets will likely continue to amplify these divisive narratives relating to Georgia's runoff election, potentially to undermine confidence in the electoral process and results.

- (U) As of late November 2020, Iranian media outlets claimed that pro-Trump rallies in Atlanta and lawsuits challenging election results could politicize the recount, sow discord, and further exacerbate social divisions. Russian media outlets focused on voting irregularities and allegations of voter fraud, amplifying the narrative that the election had been stolen from the President.

- (U) As of early June 2020, during Georgia's primary election, Russian state media highlighted claims that reductions in the number of in-person polling places and the resulting long lines disproportionately affected communities of color and suppressed their vote.

(U) Russia's Previous Targeting of Georgia during the 2016 US Presidential Election

(U//FOUO) A Russian military officer in 2016 viewed a job posting for a Georgia county election technician and visited a second Georgia county website containing general information for candidates, according to a US newspaper citing information from the state's Office of the Secretary of State. The military officer did not apply for the position, according to the same report. In addition to visiting county election websites in Georgia, Iowa, and Florida to identify vulnerabilities, this individual and other Russian military officers in 2016 exfiltrated voter data from a state board of elections website, compromised a US election vendor, and e-mailed malware to entities involved in administering elections in numerous Florida counties, according to a 2018 US DOJ indictment. We did not observe a similar effort by the Main Intelligence Directorate (GRU) during the 2020 general election.

(U) Outlook: Georgia Federal, State, and Local Agencies' Partnership a Strong Bulwark Against Potential Election Threats

(U//FOUO We remain concerned that potential violent flashpoints and foreign influence actors' likely intent to amplify divisive narratives in Georgia could foster a heightened threat environment leading up to the runoff election on 5 January 2021. In this threat environment, violent extremist or other actors could potentially continue or increase violent threats against public officials, violently clash with ideologically opposing groups, or otherwise seek to conduct violence against government or law enforcement entities. However, Georgia's federal, state, and local agencies remain well positioned to monitor, report, and mitigate potential threats to or associated with the election, based on interviews with state and federal agencies in Georgia. DHS is coordinating closely with Georgia and federal agency partners regarding operational preparations to secure the runoff election. Members of these partner agencies—in addition to DHS I&A personnel—will participate in multiple jointly staffed operations centers on the night before and the day of the runoff election to ensure the integrity and safety of the runoff election and its outcome.

- (U//FOUO) **Georgia Bureau of Investigation – Georgia Information Sharing and Analysis Center (GBI-GISAC).** The state fusion center continues to monitor and report on any incident or suspicious activity that could potentially impact Georgia's threat environment during the leadup to the runoff election by receiving, analyzing, and disseminating tips, leads, and other suspicious activity reports potentially indicative of election-related crimes with appropriate partners.

- (U//FOUO) **Georgia Secretary of State (SOS).** In addition to overseeing the election, the Georgia SOS office maintains close and continuing partnerships with DHS and other agencies to share details of any incidents that could potentially impact the election, including cyber incidents or physical threats.

- (U//FOUO) **DHS Cybersecurity and Critical Infrastructure Security Agency (CISA).** DHS CISA maintains close and continuing partnerships with Georgia state and local election officials, including providing training and resources to secure, respond to, and mitigate any physical and cyber activity that could impact Georgia's elections systems.

- (U//FOUO) **Georgia Emergency Management and Homeland Security Agency (GEMA).** GEMA partners closely with DHS and other federal, state, and local agencies to share information and provide resources necessary to respond to and mitigate physical and cyber threats.

- (U//FOUO) **Federal Bureau of Investigation (FBI).** The FBI is the lead federal agency for investigating threats to Georgia's election system and partners closely with agencies throughout the state to share information, respond to, and mitigate such threats.

- (U//FOUO) **DHS Office of Intelligence and Analysis (I&A).** I&A will continue to share cyber, physical, and foreign influence-related intelligence with federal and Georgia stakeholders to provide tactical and strategic warning of potential threats to the upcoming runoff.

(U//FOUO) Comments, requests, or shareable intelligence may be directed to DHS I&A at dhs-sps-rfi@dhs.hq.gov.

(U) Report Suspicious Activity
(U) **To report a computer security incident, please contact CISA at 888-282-0870; or go to https://forms.us-cert.gov/report. Please contact CISA for all network defense needs and complete the CISA Incident Reporting System form.** The CISA Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to CISA. An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information; unwanted disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent. (U) **To report this incident to the Intelligence Community, please contact your DHS I&A Field Operations officer at your state or major urban area fusion center, or e-mail DHS.INTEL.FOD.HQ@hq.dhs.gov.** DHS I&A Field Operations officers are forward deployed to every U.S. state and territory and support state, local, tribal, territorial, and private sector partners in their intelligence needs; they ensure any threats, incidents, or suspicious activity is reported to the Intelligence Community for operational awareness and analytic consumption.

(U) Tracked by HSEC-1.1, HSEC-1.5, HSEC-1.9, HSEC-7.1, HSEC-7.5, HSEC-7.9

(U) Source Summary Statement

(U//FOUO) We have **moderate confidence** in our judgment that Georgia faces a potentially heightened physical threat environment over the course of its US Senate election cycle due to a confluence of flashpoints, some of which sparked ideologically motived violence or threats of such violence in Georgia and nationwide during 2020. We base this judgment on a body of law enforcement reports, exchanges with fusion center analysts, and US media reporting detailing incidents of ideological violence and threats of such violence in Georgia and nationwide in 2020. However, we acknowledge that we do not have any specific, credible reporting indicating a threat specifically related to Georgia's US Senate runoff—and only fragmentary and limited reporting of election-related violence in general. Additional reporting indicating a specific threat to entities in Georgia over the next month would further bolster our confidence in this assessment.

(U//FOUO) We have **high confidence** in our judgment that incidents similar to those observed during the 2020 presidential election season—including unattributed suspicious scanning or probing of cyber networks, indirect impacts from ransomware and other cybercrime, or network disruptions not associated with malicious activity—likely could occur again during the runoff election. We base this judgment on a body of DHS I&A field reports derived from state and local election and network security officials and US media reporting focused on election network issues.

(U//FOUO) We have **high confidence** in our assessment that foreign threat actors view the national significance of Georgia's US Senate runoff election to be an opportunity to use social media and other influence tactics focused on the state. We base this judgment on a review of foreign state-run media's coverage of the runoff election, as well as previous US and foreign open source reporting indicating Iran, Russia, and other nation-state actors' continued willingness to generate misleading or false information on sensitive and divisive topics in attempts to influence US voters and undermine confidence in democratic processes.

CLASSIFICATION: **UNCLASSIFIED//FOR OFFICIAL USE ONLY**

Homeland Security

Office of Intelligence and Analysis

Customer Feedback Form

Product Title: (U//FOUO) Threat Environment Leading into US Senate Runoff Election in Georgia

All survey responses are completely anonymous. No personally identifiable information is captured unless you voluntarily offer personal or contact information in any of the comment fields. Additionally, your responses are combined with those of many others and summarized in a report to further protect your anonymity.

1. Please select partner type: Select One **and function:** Select One

2. What is the highest level of intelligence information that you receive? Select One

3. Please complete the following sentence: "I focus most of my time on:" Select One

4. Please rate your satisfaction with each of the following:

	Very Satisfied	Somewhat Satisfied	Neither Satisfied nor Dissatisfied	Somewhat Dissatisfied	Very Dissatisfied	N/A
Product's overall usefulness	○	○	○	○	○	○
Product's relevance to your mission	○	○	○	○	○	○
Product's timeliness	○	○	○	○	○	○
Product's responsiveness to your intelligence needs	○	○	○	○	○	○

5. How do you plan to use this product in support of your mission? *(Check all that apply.)*

- ☐ Drive planning and preparedness efforts, training, and/or emergency response operations
- ☐ Observe, identify, and/or disrupt threats
- ☐ Share with partners
- ☐ Allocate resources (e.g. equipment and personnel)
- ☐ Reprioritize organizational focus
- ☐ Author or adjust policies and guidelines
- ☐ Initiate a law enforcement investigation
- ☐ Intiate your own regional-specific analysis
- ☐ Intiate your own topic-specific analysis
- ☐ Develop long-term homeland security strategies
- ☐ Do not plan to use
- ☐ Other:

6. To further understand your response to question #5, please provide specific details about situations in which you might use this product.

7. What did this product *not* address that you anticipated it would?

8. To what extent do you agree with the following two statements?

	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disgree	N/A
This product will enable me to make better decisions regarding this topic.	○	○	○	○	○	○
This product provided me with intelligence information I did not find elsewhere.	○	○	○	○	○	○

9. How did you obtain this product? Select One

10. Would you be willing to participate in a follow-up conversation about your feedback? Yes

To help us understand more about your organization so we can better tailor future products, please provide:

Name:		*Position:*	
Organization:		*State:*	
Contact Number:		*Email:*	

Submit Feedback

Privacy Act Statement

From: CISA CurOps (b) (6) [redacted] <CISA.IOD.CurOps@cisa.dhs.gov>

To: CISA Daily Ops (b) (6) [redacted]
(b) (6) [redacted]
(b) (6) [redacted]

Subject: CISA Weekly Operations Infographic 4 Jan 2021

Date: 2021/01/04 07:56:25

Priority: Normal

Type: Note

UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO)

TLP: AMBER

WARNING: Information in this report is FOUO//TLP: AMBER. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm, consistent with both the DHS policy relating to safeguarding FOUO information (link here) and with the Traffic Light Protocol, http://www.us-cert.gov/tlp. Information in this report is not customarily in the public domain and may be exempt from public release under the Freedom of Information Act (5 U.S.C. § 552). Further, this section may contain or be based upon commercial or financial information, which is privileged or confidential, law enforcement sensitive, or deliberative/pre-decisional material. DHS personnel are reminded of their obligations under DHS Form 11000-6, Non-Disclosure Agreement. Further dissemination of any of the information contained in this REPORT requires express consent from the CISA CurOps.

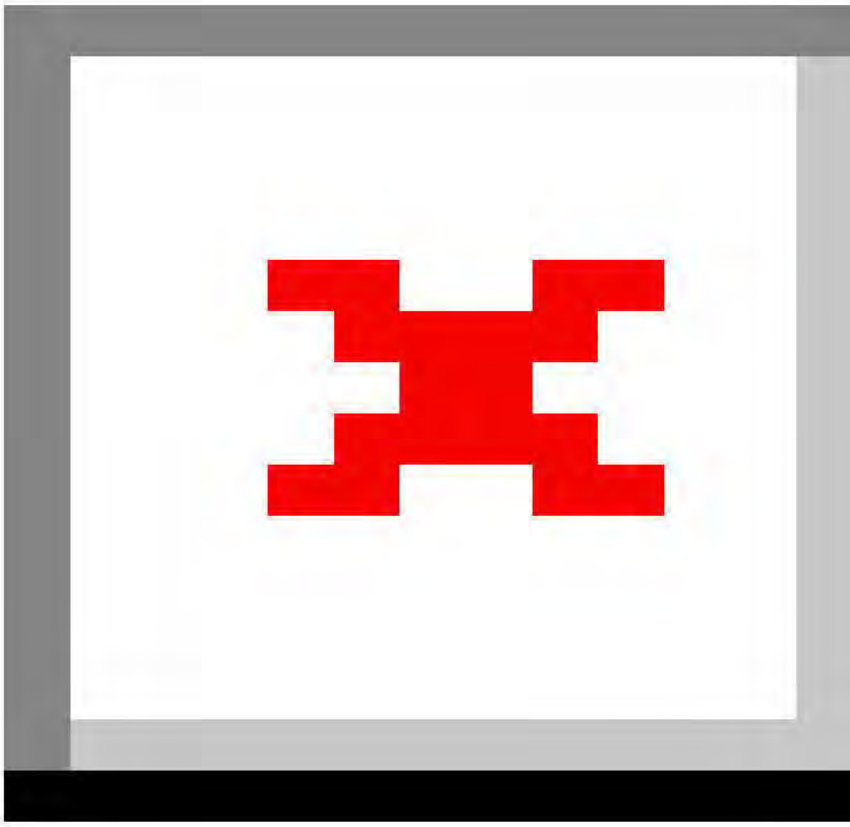
Good Morning,

Please see the attached CISA Ops Infographic for the week of 4 Jan.

Respectfully,

CISA Current Operations
Cybersecurity and Infrastructure Security Agency (CISA)
Office: (b) (6) [redacted] | Email: (b) (6) [redacted]

cid:image002.png@01D62213.AAB10820



Graphical user interface, text, application Description automatically generated

TLP: AMBER

Sender:	CISA CurOps (b) (6) (b) (6) (b) (6)
Recipient:	CISA Daily Ops (b) (6) (b) (6) (b) (6)
Sent Date:	2021/01/04 07:55:47
Delivered Date:	2021/01/04 07:56:25

DIRECTOR'S WEEKLY OPERATIONS INFOGRAPHIC

January 4, 2021

CISA CENTRAL
202.282.9201

ALERT LEVELS

NTAS	None	Bulletin	Elevated	Imminent
NOC	Steady State	Awareness	Guarded	Concern	Urgent

OPERATION & SITUATION UPDATES

COVID-19

- COVID-19 statistics: US Total cumulative cases are 20,346,272 million with 349,246 deaths
- New cases in the last 7 days: 1,436,462
- New deaths in the last 7 days : 18,345
- The United Kingdom became first nation to administer the Oxford-AstraZeneca vaccine.
- As of 2 Jan, there have been 13 million vaccine doses distributed and 4.2 million vaccine doses administered in the US

Georgia Senate Runoff Elections - 5 JAN

- Polls open at 0600 EST.
- Region IV personnel will work in close coordination with election officials and public/private sector partners across the region to monitor in-person voting activities, supporting cyber systems, and physical sites.

ENGAGEMENTS

- 11 JAN: AD Brown and DAD DeLaurentis will participate in the SAFECOM & the National Council of Statewide Interoperability Coordinators Bi-weekly Sync.
- 11 JAN: AD Brown will participate in the Monthly Board Meeting with FirstNet Management.
- 13 JAN: AD Brown will speak at the Consumer Electronics Show on Mitigating Emergency Communications Impacts During A Global Pandemic.

CONGRESSIONAL AFFAIRS

- No Scheduled Events

INTERNATIONAL AFFAIRS

- No Scheduled Events

	(A)DIR	(A)D/DIR	COS	(A)DAD ISD	(A)AD CSD	AD ECD	AD IOD	AD SED	AD NRMC
Today	NCR	NCR	NCR	NCR	NCR	NCR	NCR	NCR	NCR
Tomorrow	NCR	NCR	NCR	NCR	NCR	NCR	NCR	NCR	NCR

From: Scully, Brian (b) (6) (b) (6) (b) (6) >

To: Hale, Geoffrey (b) (6) (b) (6) <Geoffrey.Hale@cisa.dhs.gov>

CC: Snell, Allison (b) (6) (b) (6)

Subject: GA Disinfo

Date: 2021/01/04 09:43:31

Priority: Normal

Type: Note

Hey Geoff,

Attached is last week's Weekly CFI Brief from the ByLight team. (b) (5) e. Will keep you posted on anything else we come across.

Brian

Sender: Scully, Brian (b) (6) P (b) (6)

Recipient: Hale, Geoffrey (b) (6) (b) (6) (b) (6) Snell, Allison (b) (6) (b) (6)

Sent Date: 2021/01/04 09:42:37

Delivered Date: 2021/01/04 09:43:31

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

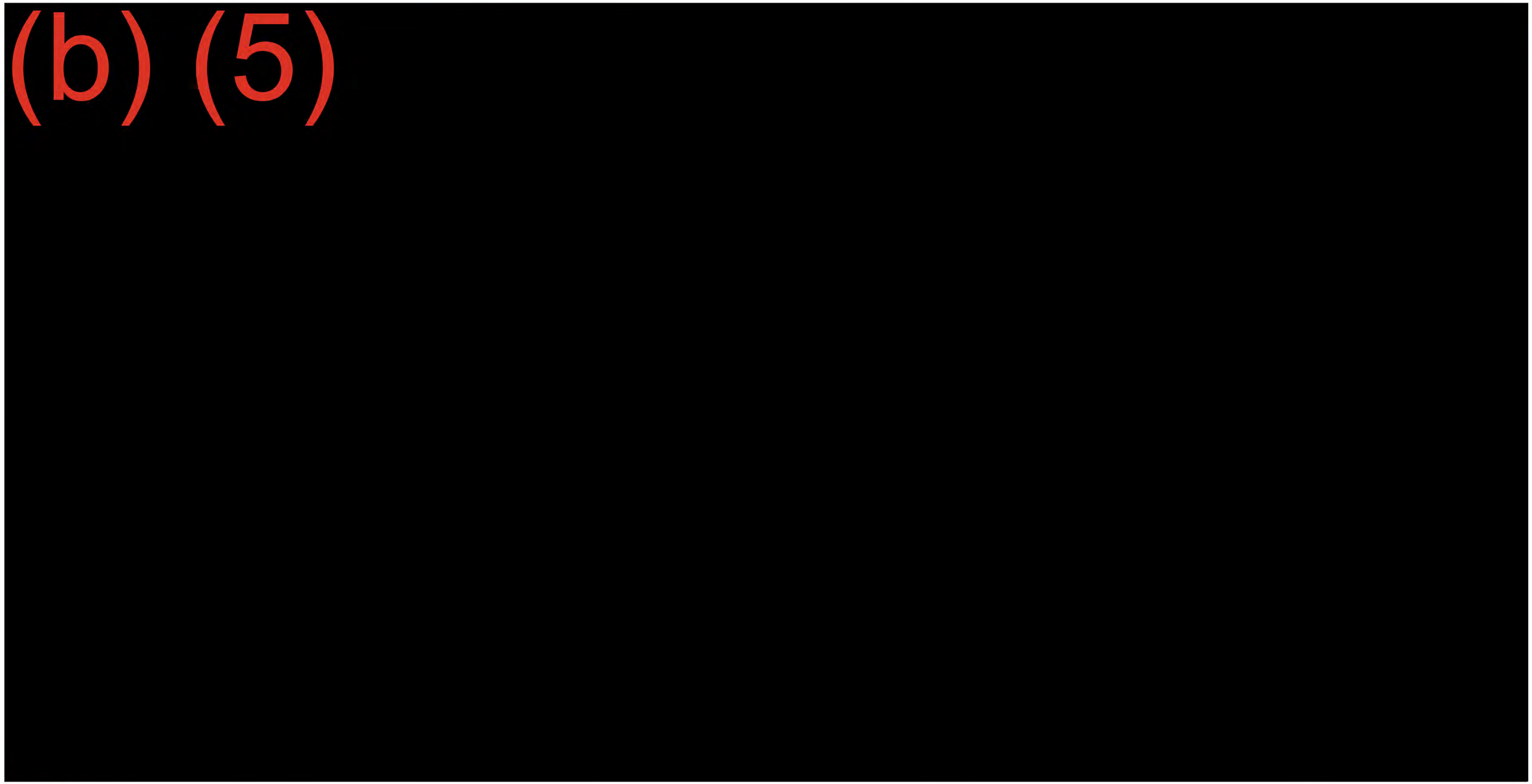
(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)



(b) (5)

(b) (5)

(b) (5)

(b) (5)

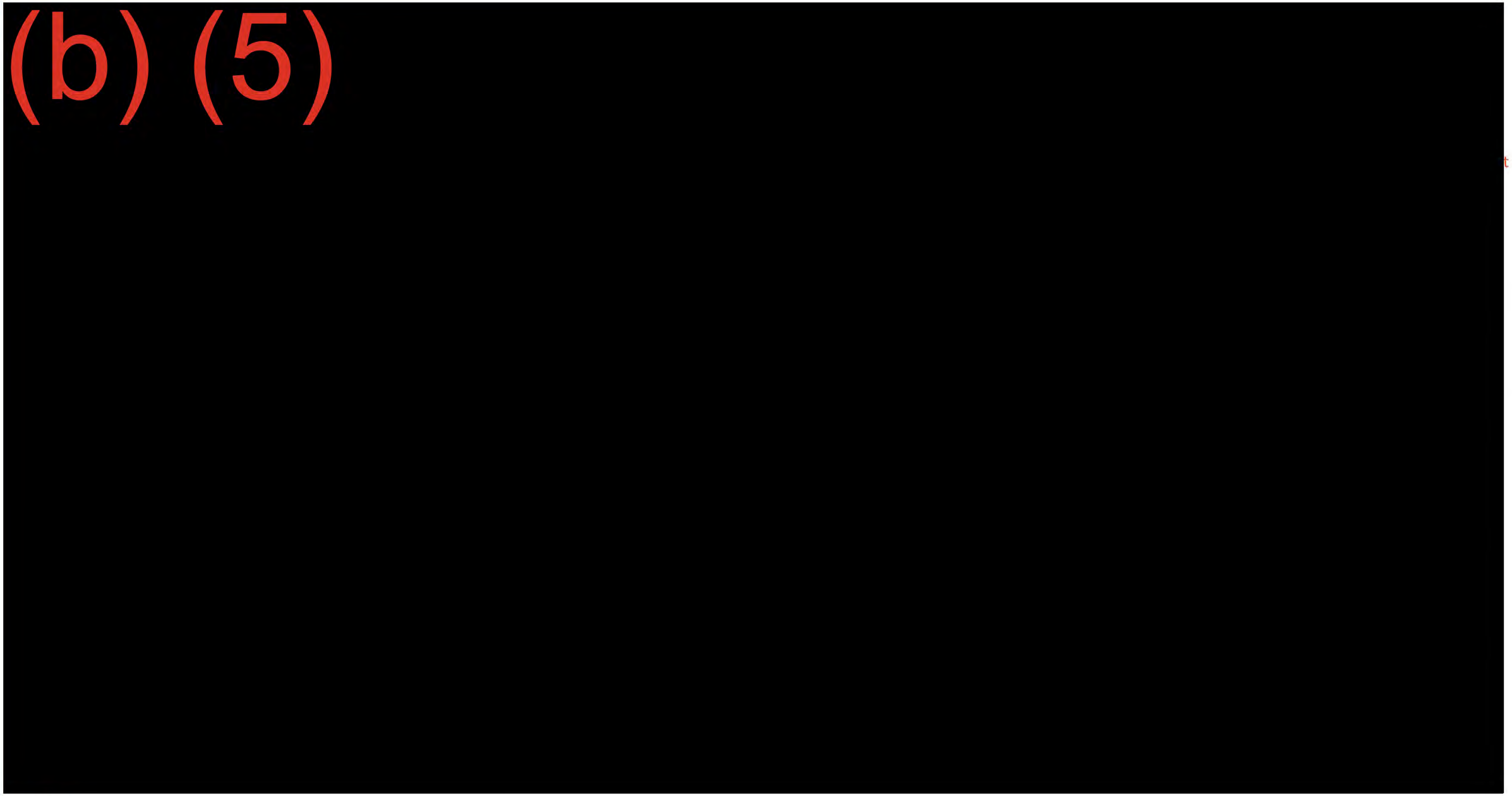
(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)



(b) (5)

(b) (5)