CYBER THREAT RESPONSE MEMORANDUM

MEM 2016-013
3 August 2016

(b)(3) Foreign States Leaking Data To Influence US Political Process

(U) This is an IC-Coordinated Memorandum

Memorandum For: (b)(3), (b)(6)
Cybersecurity Coordinator
National Security Council

From: Tonya Ugoretz
Director
Cyber Threat Intelligence Integration Center

(C//NF) This memorandum was prepared under the auspices of the Cyber Threat Intelligence Integration Center (CTIIC) and drafted by CIA's Center for Cyber Intelligence and CTIIC. It was coordinated with CIA and NIO/Cyber. Questions about this memo may be directed to the D/CTIIC on secure (b)(3) or unsecure (b)(3)

(b)(3)

(b)(1), (b)(3), (b)(7)(E)

(b)(3) Foreign States Leaking Data To Influence US Political Process

(U) This is an IC-coordinated memorandum.

(b)(1), (b)(3) Foreign adversaries probably have access to a wide range of data that they could leak to try to influence the US election cycle; (b)(1), (b)(3)

- (b)(1), (b)(3) Russia has the capability and probably the intent to use cyber-enabled data leaks to influence the US political process based on its probable involvement in the leak in June of Democratic National Committee (DNC) documents,[12] its broad access to US data, and its history of interfering in foreign elections.[34]
- (b)(1), (b)(3)
- (b)(1), (b)(3)

(b)(3) Any such future operation to discredit key individuals could use information related to family members, political allies, and other key contacts or affiliated organizations.

(b)(1), (b)(3)

(b)(3) (b)(1), (b)(3)

(b)(1), (b)(3)

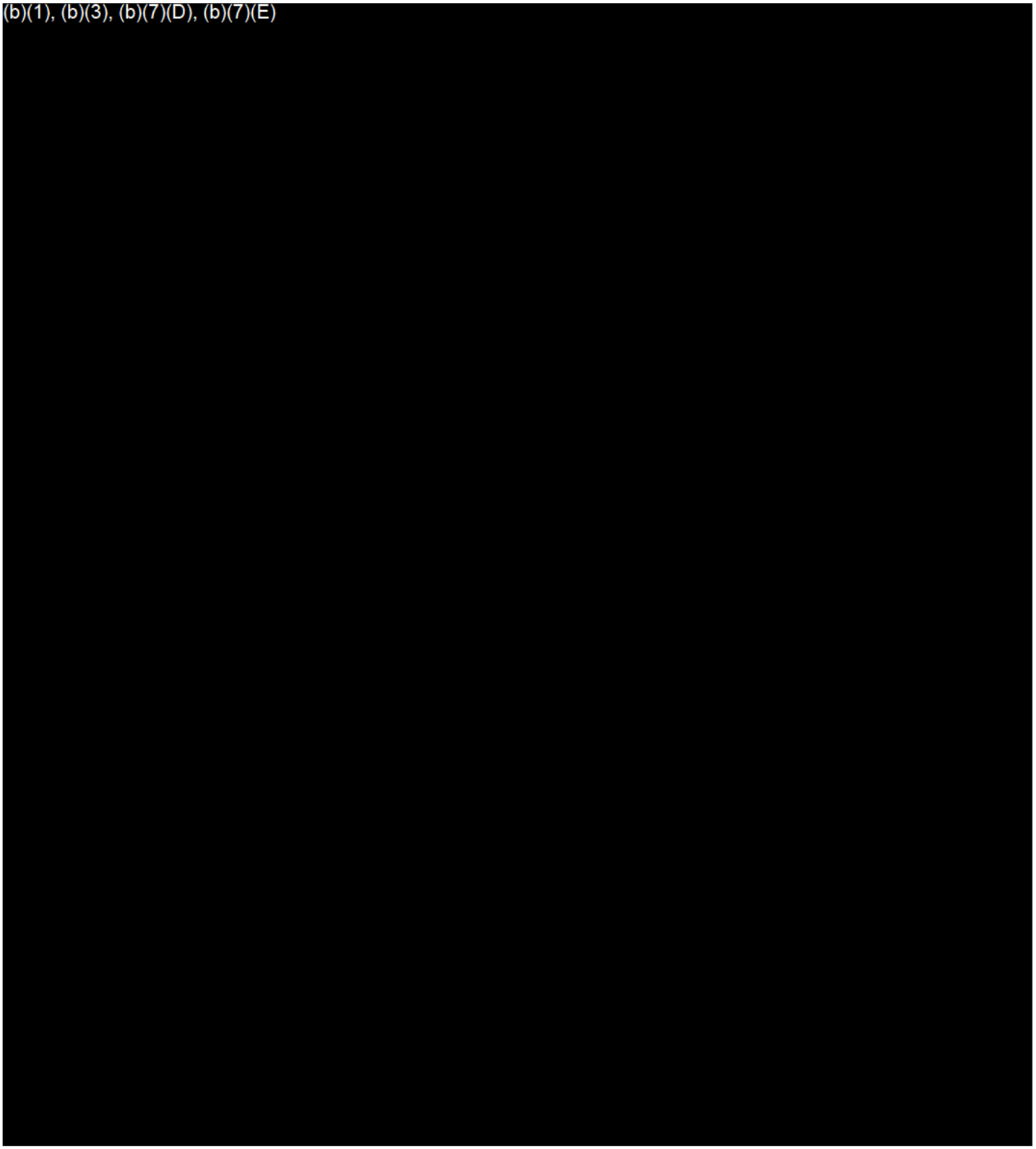
(b)(3) Early detection would provide a potential opportunity for US messaging to shape how the information is interpreted before the disclosure. For example, the online persona Guccifer 2.0—probably used by Russian intelligence services—publicly announced the transfer of DNC e-mails and files to WikiLeaks more than a month before the e-mails were posted to the website, (b)(3) (b)(3) Other activities that might indicate a state is contemplating the release of stolen data to influence a foreign election include:

- Specific directions to interfere in an election;
- A surge in intrusion activity against politically sensitive networks in the runup to an election; and
- An increase in government commentary and state-controlled media reporting that is critical of a candidate or policy position.

(b)(3) Disinformation Operations Versus Data Leaks

(b)(1), (b)(3), (b)(7)(E)

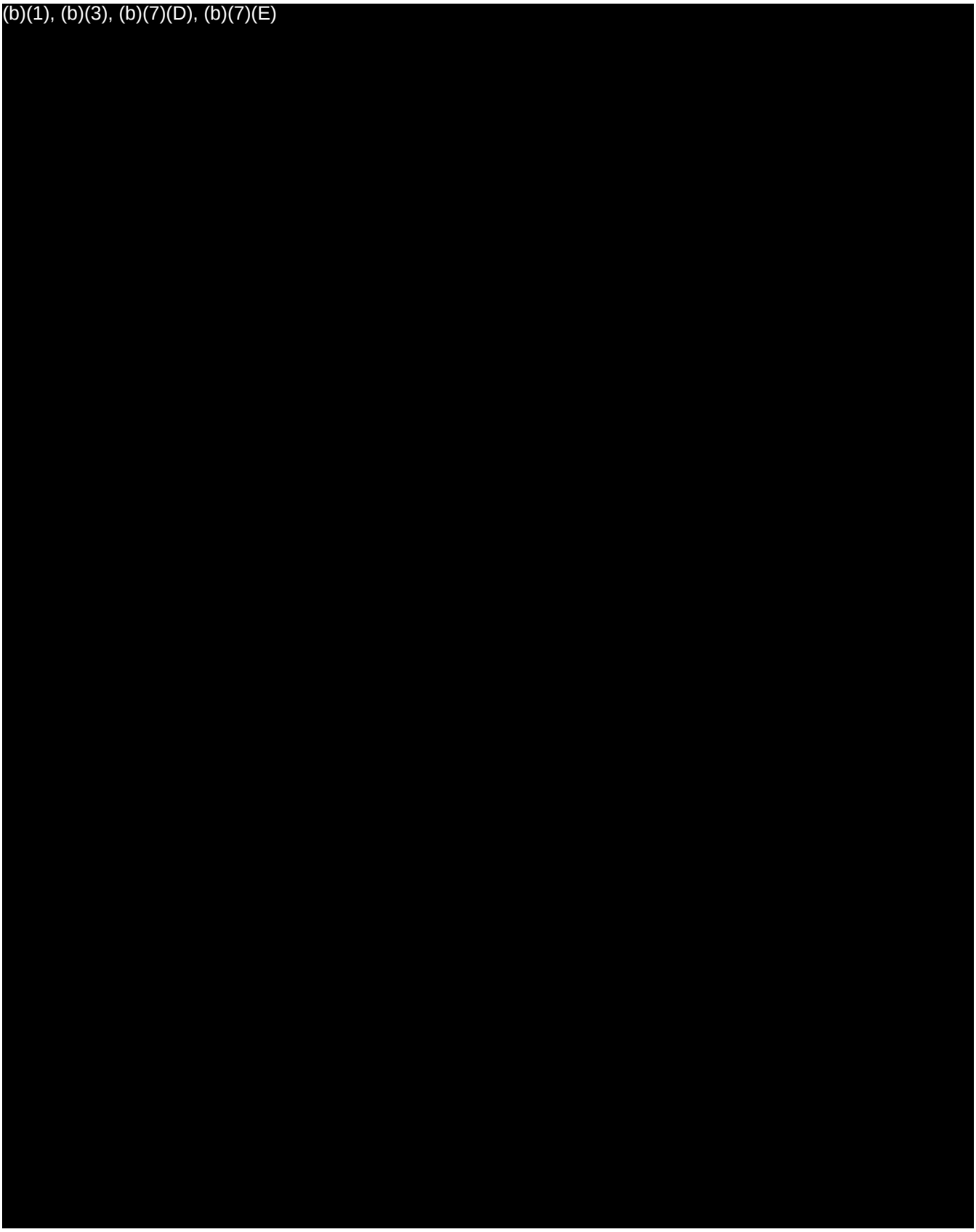
(b)(1), (b)(3), (b)(7)(D), (b)(7)(E)



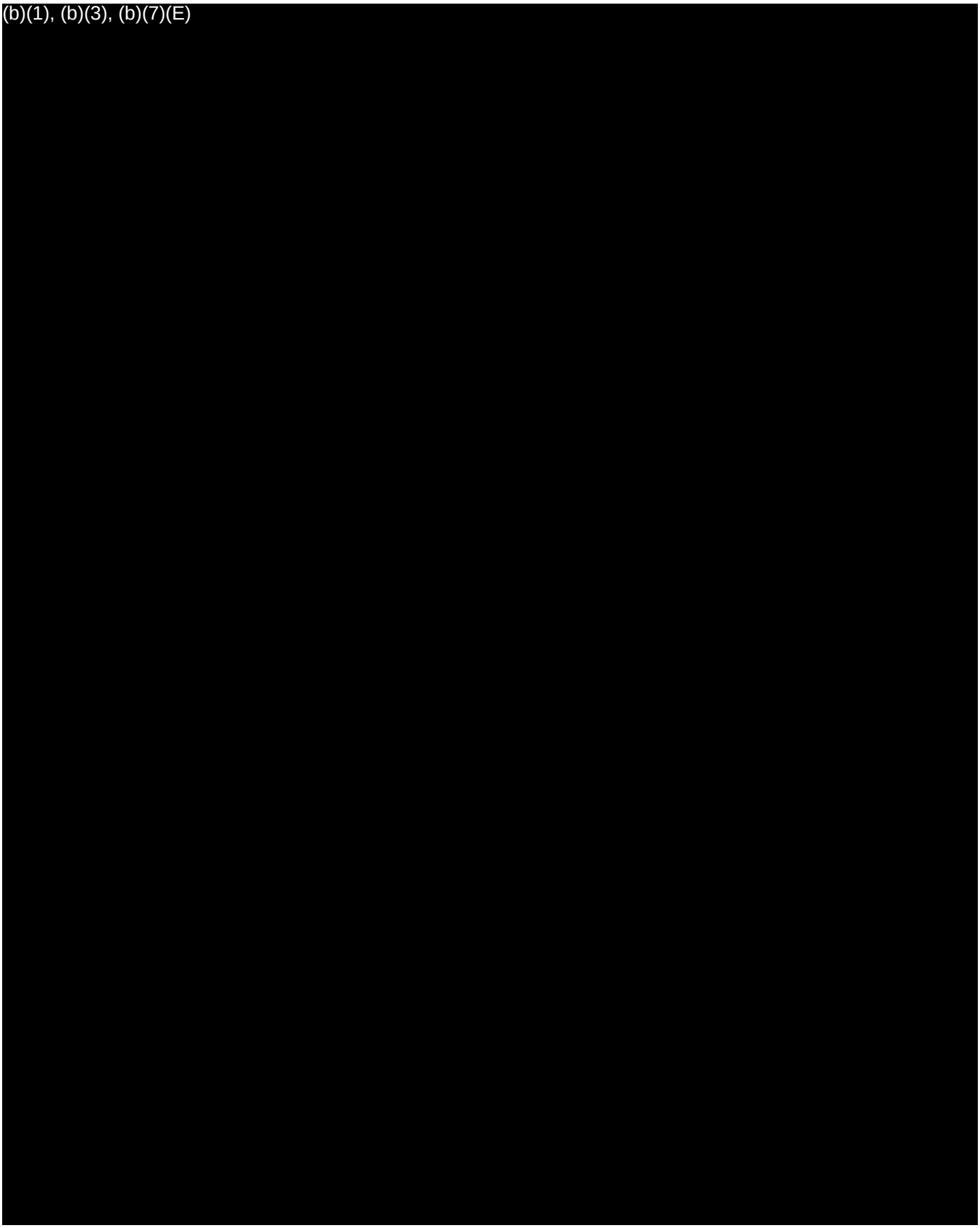
(U) Sources

(b)(1), (b)(3), (b)(7)(E)

(b)(1), (b)(3), (b)(7)(D), (b)(7)(E)



(b)(1), (b)(3), (b)(7)(E)



(b)(1), (b)(3), (b)(7)(E)