
From: (b) (6)
Sent: 1/10/2023 8:16:02 AM
To: Office of the President of Ukraine [office.president@ukr.net]
CC: (b) (6) ayermak@zelenskyy.team
Subject: RE: President of Ukraine - Chairman Powell (FRS). Request

NONCONFIDENTIAL // EXTERNAL

Dear Kyrylo,

We are in receipt of the request and will revert back.

Best regards,

(b) (6)



(b) (6)
Assistant to the Chair
The Honorable Jerome H. Powell
Federal Reserve Board of Governors
William McChesney Martin, Jr. Building
2001 C Street, N.W.
Washington, D.C. 20551
(b) (6) Office
(b) (6)

From: Office of the President of Ukraine <office.president@ukr.net>
Sent: Tuesday, January 10, 2023 8:12 AM
To: (b) (6)
Cc: (b) (6) >; ayermak@zelenskyy.team
Subject: President of Ukraine - Chairman Powell (FRS). Request

NONCONFIDENTIAL // EXTERNAL

Dear (b) (6)

President of Ukraine Volodymyr Zelenskyy would like to have a conversation with Chairman of the Federal Reserve System Honorable Jerome Powell.

President Zelenskyy would like to personally congratulate him with recent holidays and discuss common issues and plans:

The impact of the war in Ukraine on the world economy for the coming year,
Forecasts on the economic situation in the world;

A few days ago, President Zelensky had a productive conversation with President of the European Central Bank, Christine Lagarde to understand the general situation in the European economy. In this regard the President believes that it would be extremely useful for him to have a similar conversation with Honorable Jerome H. Powell.

We are ready to organize a video (Zoom, Webez) or telephone conversation at any time convenient for your side.

I will wait for your response.

With best regards,
Kyrylo Tymoshenko
Deputy Head of the office
Office of the President
of Ukraine
11 Bankova str, Kyiv
Tel.:+380 (44)290-77-55
+48222304009

Dear Kyrylo,

Thank you for your kind message.

As regards the contacts for Chair Powell, you can reach out to his assistant:

(b) (6)

Assistant to the Chairman
The Honorable Jerome H. Powell
Federal Reserve Board
Marriner Eccles Board Building
20th and C Streets, N.W.
Washington, D.C. 20551
Phone: (b) (6)

(b) (6)

Kindly copy also her colleague, (b) (6)

Kind regards and all the best

(b) (6)



(b) (6)

(b) (6)

European Central Bank
Sonnemannstrasse 20
60314 Frankfurt am Main

Tel : (b) (6)

Fax : (b) (6)

Office e-mail: (b) (6)

Personal e-mail: (b) (6)

<http://www.ecb.europa.eu>

From: Office of the President of Ukraine <office.president@ukr.net>

Sent: 10 January 2023 08:23

To: Office President (b) (6)

Cc: ayermak@zelenskyi.team; Lagarde, Christine (b) (6)

Subject: [EXT] Re: RE: RE: RE: RE: RE: RE: RE: President of Ukraine - President Lagarde. Request

Dear (b) (6)

Thank you again for the help with last conversation of our Presidents.

We have one more question. As you are in touch could you give us please right contacts of the office of Chair of the Federal Reserve Jerome Powell or connect us with his office?

President also hope to talk to him.

Let us know if it's possible.

Thank you!

Best,

Kyrylo Tymoshenko
Deputy Head of the office

Office of the President
of Ukraine
11 Bankova str, Kyiv
Tel.: [+38\(044\)290-77-55](tel:+38(044)290-77-55)

<http://president.gov.ua>

SAVE PAPER - THINK BEFORE YOU PRINT

From: (b) (6)
Sent: 1/10/2023 11:46:32 AM
To: Office of the President of Ukraine [office.president@ukr.net]
CC: ayermak@zelenskyy.team; (b) (6)
Subject: RE: RE: RE: President of Ukraine - Chairman Powell (FRS). Request

NONCONFIDENTIAL // EXTERNAL

Dear Kyrylo,

Thank you, I have noted that this will be a one-on-one call.

Best regards,

(b) (6)

From: Office of the President of Ukraine <office.president@ukr.net>
Sent: Tuesday, January 10, 2023 11:44 AM
To: (b) (6)
Cc: ayermak@zelenskyy.team; (b) (6)
Subject: Re: RE: RE: President of Ukraine - Chairman Powell (FRS). Request

NONCONFIDENTIAL // EXTERNAL

Dear (b) (6)

Thank you! We received the link. There will be only technical assistant in the beginning to check the connection. Then only the President will be on the line.


With best regards,
Kyrylo Tymoshenko

NONCONFIDENTIAL // EXTERNAL

Dear Kyrylo,

Below is the link for the (b) (7)(E). Will staff join the call?

(b) (7)(E)





Thanks,

(b) (6)

From: Office of the President of Ukraine <office.president@ukr.net>

Sent: Tuesday, January 10, 2023 10:58 AM

To: (b) (6)

Cc: ayermak@zelenskyy.team; (b) (6)

Subject: Re: RE: President of Ukraine - Chairman Powell (FRS). Request

NONCONFIDENTIAL // EXTERNAL

Dear (b) (6)

Thank you for your quick response and Chair Powell's readiness to talk.

January 19 9:00 ET (Washington time) is convenient for President Zelenskyy.

We will be waiting for a (b) (7)(E) invitation link from you.

Thanks for the help!

With best regards,

Kyrylo Tymoshenko

NONCONFIDENTIAL // EXTERNAL

Dear Kyrylo,

Chair Powell is on travel this week. He is available the following times below to have a telephone conversation via (b) (7)(E) with President Zelenskyy. Please let me know what will work in the schedule and I will provide the (b) (7)(E) link.

January 17 9:00 am ET

January 19 9:00 am ET

January 20 9:00 am ET

Best regards,

(b) (6)

From: (b) (6)
Sent: 1/19/2023 7:55:05 AM
To: Office of the President of Ukraine [office.president@ukr.net]
CC: ayermak@zelenskyy.team; (b) (6) (b) (6)
Subject: Re: Re[2]: Possible to reschedule call with Federal Reserve Chair today?

PERSONAL/NONWORK // EXTERNAL

Thank you. We look forward to rescheduling. (b) (6) will be in touch.
Warmly,
(b) (6)

From: Office of the President of Ukraine <office.president@ukr.net>
Sent: Thursday, January 19, 2023 7:53 AM
To: (b) (6)
Cc: ayermak@zelenskyy.team <ayermak@zelenskyy.team>; (b) (6) (b) (6)
(b) (6)
Subject: Re[2]: Possible to reschedule call with Federal Reserve Chair today?

NONCONFIDENTIAL // EXTERNAL

Dear (b) (6)

Thank you for your condolences. The loss of the Minister in such a difficult time of war is a serious shock for us.

President Zelenskyy wishes Chair Powell a speedy recovery.

Of course, let's move this conversation to a more favorable time. We will be waiting for a new date and time for him from you.

Also I know that this conversation is very important for President Zelenskyy and we are ready to arrange it at a convenient time for Chair Powell as soon as possible.

With best regards,
Kyrylo Tymoshenko
Deputy Head of the office
Office of the President
of Ukraine
11 Bankova str, Kyiv
Tel.:+380 947100320
+48222304009

From: (b) (6)
Sent: Thursday, January 19, 2023 7:35 AM
To: office.president@ukr.net <office.president@ukr.net>; (b) (6) (b) (6)

(b) (6)

Subject: Possible to reschedule call with Federal Reserve Chair today?

Dear Kyrylo,

As was announced yesterday, Chair Powell has tested positive for COVID. He is very much looking forward to talking with President Zelensky but would appreciate it if the call today could be postponed. He sends his deepest condolences for the deaths of Interior Minister Monastyrsky and others in the horrific crash this week and his admiration and solidarity with you and the Ukrainian people. We will work to reschedule the call as soon as possible. Thank you for your understanding.

Sincerely,

(b) (6)

(b) (6)

Federal Reserve Board

(b) (6)

Duplicate

From: (b) (6)
Sent: 1/19/2023 10:24:41 AM
To: Office of the President of Ukraine [office.president@ukr.net]
CC: ayermak@zelenskyy.team; (b) (6) (b) (6)
(b) (6); (b) (6)
Subject: RE: RE: Re[2]: Possible to reschedule call with Federal Reserve Chair today?

NONCONFIDENTIAL // EXTERNAL

Dear Kyryllo,

I am confirming the meeting with Chair Powell and President Zelenskyy for Tuesday, January 24, 8:00 am – 8:30 am (DC time). This will be a one-on-one meeting. The (b) (7)(E) link to come.

Best regards,

(b) (6)

From: Office of the President of Ukraine <office.president@ukr.net>
Sent: Thursday, January 19, 2023 9:01 AM
To: (b) (6)
Cc: ayermak@zelenskyy.team; (b) (6)
Subject: Re: RE: Re[2]: Possible to reschedule call with Federal Reserve Chair today?

NONCONFIDENTIAL // EXTERNAL

Dear (b) (6),

Tuesday, January 24 8:00 am (Washington time) is convenient for President Zelenskyy.

We will be waiting for a (b) (7)(E) invitation link from you.

Thank you.

Best,
Kyryllo

NONCONFIDENTIAL // EXTERNAL

Dear Kyrylo,

Please let me know if any of the following times will work for Chair Powell and President Zelenskyy to speak.

Monday, January 23, 8:30 am – 9:30 am

Tuesday, January 24, 8 am – 8:30 am

Wednesday, January 25, 8 am – 9 am

Best regards,

(b) (6)

Duplicate

From: Office of the President of Ukraine [office.president@ukr.net]
Sent: 1/27/2023 6:59:23 AM
To: (b) (6)
CC: ayermak@zelenskyy.team; (b) (6)
Subject: Re[2]: RE: RE: Re[2]: Possible to reschedule call with Federal Reserve Chair today?

NONCONFIDENTIAL // EXTERNAL

Dear (b) (6),

President Zelenskyy would like to thank Chair Powell once again for this important conversation for us and express gratitude for his professionalism.

We have a small request.

Could you connect us with Secretary of the Treasury Janet Yellen so that President Zelenskyy could discuss the economic situation with her directly.

President Zelenskyy would like to hold this conversation informally, without the attention of the press. Therefore, we thought that through you it would be fast and confidential.

With best regards,
Kyryllo Tymoshenko
Deputy Head of the office
Office of the President
of Ukraine
11 Bankova str, Kyiv
Tel.:+380 947100320
+48222304009

Thank you! We received the link.

Best,
Kyryllo

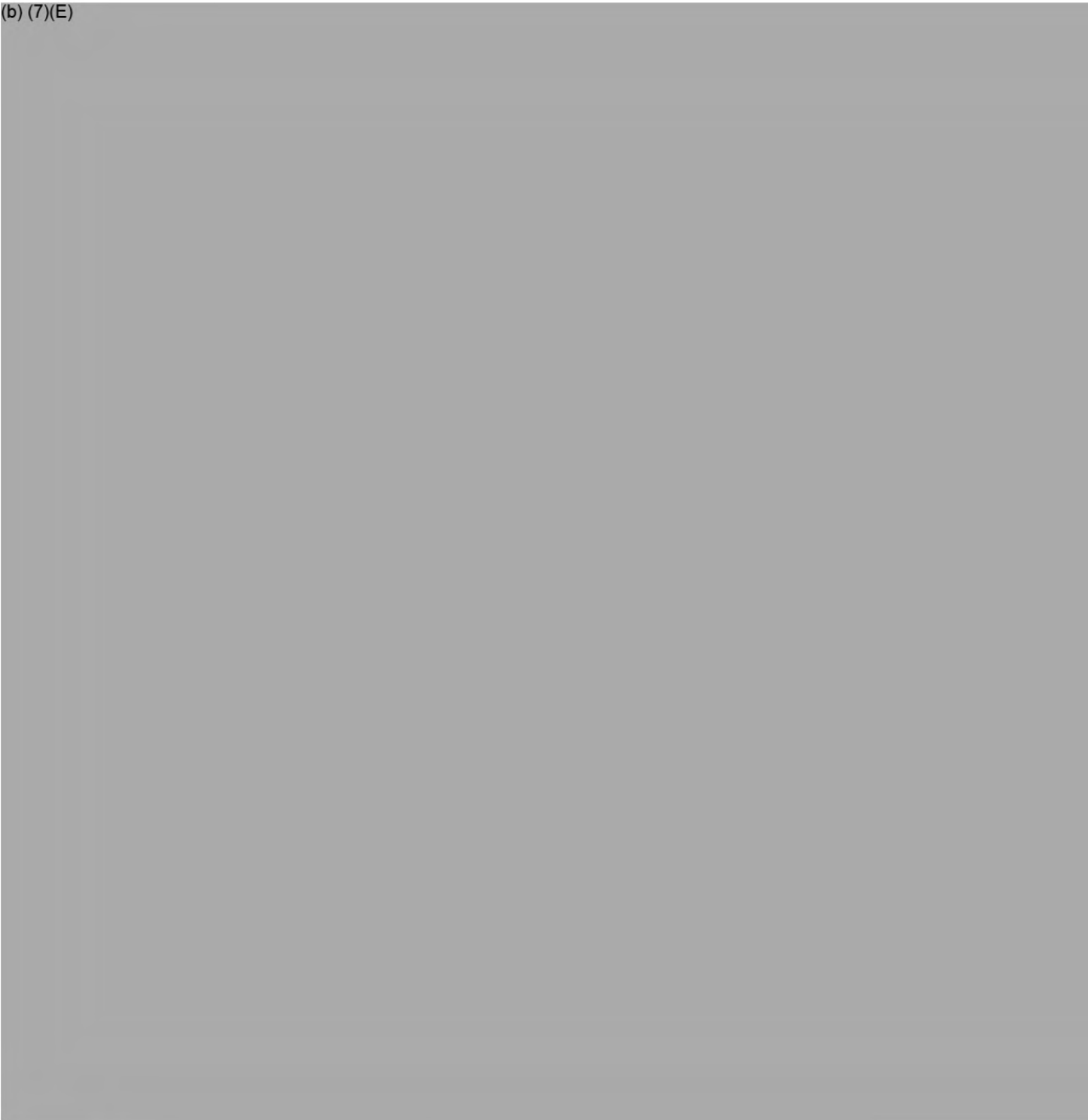
NONCONFIDENTIAL // EXTERNAL

Dear Kyryllo,

Below is the new (b) (7)(E) link for the meeting on Tuesday, January 24, 8:00 am – 8:30 am (DC time)

(b) (7)(E)

(b) (7)(E)



Best,

(b) (6)

From: (b) (6)
Sent: 2/10/2023 10:42:02 AM
To: Office President (b) (6)
Subject: RE: FW: President of Ukraine - Chairman Powell (FRS). Request

NONCONFIDENTIAL // EXTERNAL

Thanks (b) (6), this is helpful.

From: Office President (b) (6)
Sent: Friday, February 10, 2023 10:35 AM
To: (b) (6)
Cc: Office President (b) (6)
Subject: RE: FW: President of Ukraine - Chairman Powell (FRS). Request

NONCONFIDENTIAL // EXTERNAL

Dear (b) (6),

Thanks for asking.

The issue is a bit hairy. We were in touch with Mr Tymoshenko and a video call between President Zelenskyy and Madame Lagarde took place on 6th January.

He then requested other contacts (among which the one of Chair Powell) and I gave him the office contact, so yours.

But in the meantime, we got to know that Mr Tymoshenko left the office of President Zelenskyy https://en.wikipedia.org/wiki/Kyrylo_Tymoshenko

and moreover, he wrote us an e-mail in which he stated: President Zelenskyy had a very productive conversation with Chair Powell.

Chair Powell also conveyed his best wishes to President Lagarde.

So I assume this is not true?

Seen that Mr Tymoshenko now left the office of President Zelenskyy and all the above, I would be extra cautious when handling his request...

Hope this helps.

Kind regards

(b) (6)

From: (b) (6)
Sent: 10 February 2023 16:20
To: Office President (b) (6)
Subject: [EXT] FW: President of Ukraine - Chairman Powell (FRS). Request

NONCONFIDENTIAL // EXTERNAL


Dear (b) (6)

I just want to confirm that the email below (see trail) is a legitimate email from you and that a phone call with President Zelenskyy did occur from your office.

Best regards,

(b) (6)

Duplicate



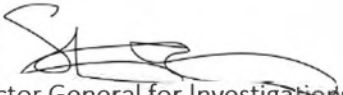


Office of Inspector General
Board of Governors of the Federal Reserve System
Consumer Financial Protection Bureau

MEMORANDUM

DATE: November 28, 2023

TO: Case File

FROM: Stephen Carroll 
Associate Inspector General for Investigations

SUBJECT: Closing of 23-0010-P

Executive Summary

On February 14, 2023, the Office of Inspector General initiated a complaint evaluation based on a referral from the Board of Governors of the Federal Reserve System that was received on February 10, 2023.¹ The referral stated that a (b) (7)(E) meeting occurred on January 24, 2023, between Board Chair Jerome Powell and an impersonator who was believed at the time to be Ukrainian President Volodymyr Zelenskyy. After the meeting, the impersonator asked for contact information for (b) (6); (b) (7)(C) , which Board staff subsequently provided.

The purpose of this investigation was to determine whether any criminal statutes, regulations, or agency policies within our jurisdiction were violated. The investigation focused on what transpired leading up to and during the January 24 meeting, including the acts of the Zelenskyy impersonator and the Board's process for scheduling communications with foreign officials.

Shortly after initiating this investigation, we learned that Board Information Security Operations and the Federal Reserve System National Incident Response Team were concurrently working on this matter.

We have found no violations of law, regulation, or policy associated with this matter. As a result, we referred these investigative findings to the OIG's Office of Information Technology (OIT). In light of our referral and as part of its 2023 audit of the Board's information security program, required by the Federal Information Security Modernization Act of 2014, OIT tested select security controls for (b) (7)(E). The testing identified improvements needed in security assessment and authorization processes, security configurations for (b) (7)(E) , and the monitoring of (b) (7)(E) communications. In addition, the testing identified an opportunity for the Board to develop a baseline of (b) (7)(E) meetings

¹ The complaint evaluation became a preliminary investigation on March 15, 2023.

with foreign officials to assist in overall security monitoring efforts. Based on the review, the Board has taken actions to strengthen security controls for (b) (7)(E). OIT plans to issue a restricted audit report detailing the results of its testing of (b) (7)(E) to include specific recommendations, by the end of 2023.

Investigative Activities

To investigate this matter, we conducted extensive email reviews, including the January 10, 2023, email sent to the Board making the initial contact on behalf of the impersonator; the emails of anyone who was involved in planning or scheduling the meeting; and the emails of any individuals who were notified of the planned meeting. This review focused on emails dated from January 10, 2023, to February 24, 2023.

We also interviewed 11 Board employees from the divisions of International Finance (IF), Monetary Affairs, and Board Members, including Chair Jerome Powell and (b) (6), (b) (7)(C) [REDACTED].²

Findings

The following sections discuss the scheduling of the meeting between Chair Powell and the impersonator, the meeting itself, the Board's role in vetting foreign contacts, the release of a video from the meeting, and the program for security of FOMC information.

Scheduling of Meeting With Chair Powell

Based on our interviews, we learned that no single person or group was solely assigned to verify the identity of foreign individuals who contact the Board to request to communicate with Board members or senior Board officials. Generally, the chair and other senior Board officials have long-standing relationships with their international counterparts, and one-on-one communications tend to be with individuals well known to the chair or to senior Board officials. We learned that before a communication with a foreign official, Board staff contacts their Treasury counterparts for information and coordination. This outreach to Treasury, however, does not involve verification of the identity of the individual requesting to communicate with the senior Board official. The Board does not have a process to regularly include other outreach to external agencies or organizations, such as the U.S. Department of State, embassies, or the White House to verify the identities of these requestors. Further, Board Information Security Operations and the Board's Integrated Resiliency and Intelligence Programs are not regularly involved in the vetting, scheduling, and logistics processes for communications between senior Board officials and foreign officials.

Through our interviews, we learned that a rare set of factors led to the January 24 meeting. First, the Board relied on a referral from the European Central Bank, which detailed President Christine Lagarde's communication with the Zelenskyy impersonator, believed at the time to be President Zelenskyy. IF

² (b) (6), (b) (7)(C) [REDACTED]

coordinated with Treasury, and all felt comfortable with Chair Powell meeting the individual claiming to be Zelenskyy because President Lagarde had just met with the individual. Second, Chair Powell joined the January 24 meeting from home while recovering from an illness. Under normal circumstances, he would have taken the meeting from his office, accompanied by an off-camera Board staff member taking notes. Third, while Chair Powell has preexisting relationships with most foreign officials with whom he meets, he did not have one with President Zelenskyy.

Meeting on January 24, 2023

Chair Powell's meeting with the Zelenskyy impersonator lasted about 30 minutes. Chair Powell started the conversation by informing the impersonator that the Federal Reserve cannot assist Ukraine directly; assistance would instead need to come from Treasury and the White House. The impersonator acknowledged that and stated that he wanted to hear from Chair Powell on the U.S. and global economies. Chair Powell believed the impersonator to be briefed and knowledgeable based on his questions. Chair Powell stated that the impersonator may have been reading information from a screen during their conversation. Chair Powell did note that the impersonator appeared to be more fluent in English than he would have expected. Chair Powell stressed that he was neither asked about nor shared anything confidential. The impersonator asked for Chair Powell's opinion on how the current head of the Central Bank of the Russian Federation was doing and his thoughts on Russia avoiding sanctions. Chair Powell responded by noting that Elvira Nabiullina is well thought of and well respected, and he did not offer any specifics on Russia's avoidance of sanctions beyond what had been publicly reported. The impersonator did not ask for any money, papers, documents, or other things of value during the conversation.

Board's Role in Vetting Foreign Contacts

Chair Powell stated that IF is responsible for ensuring that foreign officials requesting to communicate are properly verified and vetted. Chair Powell reiterated that this one-on-one meeting with the Zelenskyy impersonator was extremely unusual given that nearly all of his communications are with people he is already deeply familiar with. Chair Powell explained that in the future, if someone at the Board were to be contacted by a foreign official with which the chair does not have a preexisting relationship, a simple fix would entail an individual from the Board calling the relevant embassy to verify the contact. He noted that Treasury called the Ukrainian embassy on February 8, 2023, and embassy staff were able to quickly identify as false the communication request made by email for President Zelenskyy.

We were informed by multiple Board staff members that attention to detail regarding incoming email is crucial and that staff members are taking a closer look at senders' email addresses and verifying contacts as necessary. In addition, the Division of Information Technology's Technology Systems and Services imaged a new computer for Chair Powell. This step was taken as a precaution given that the preliminary forensic assessment conducted by Board Information Security Operations showed that no hacking or infiltration occurred, and, therefore, that no further action was warranted.

This document is property of the Office of Inspector General and may not be copied or disclosed without the permission of the Office of Inspector General. Appropriate safeguards should be provided for the information contained herein. Public disclosure of this information is determined by the Freedom of Information Act, title 5, U.S.C. § 552, and the Privacy Act, title 5, U.S.C. § 552a.

Video Release

A video of the call between Chair Powell and the Zelenskyy impersonator was released on April 26, 2023, to Rutube, a public Russian video platform. We have reviewed the full video and the small video segments and cannot determine whether the video has been altered. In the video, Chair Powell stated the following: “The market is already pricing in two more quarter percentage point rate hikes. We’ll look around after we make those two and we’ll say should we do any more, and then the question will be, how long do we keep rates at this level, and I think we’ll keep them there for quite some time.”

Program for Security of FOMC Information

We interviewed (b) (6), (b) (7)(C) to obtain his view on whether Chair Powell’s statement in the video constituted confidential FOMC information.³ (b) (6), (b) (7)(C) stated that Chair Powell’s statements in the video “give at least an appearance of looking like Class 1” FOMC information. We conducted a subsequent interview of Chair Powell concerning his statement in the video. Chair Powell acknowledged making the statement but noted that he did not think the statement met the definition of confidential FOMC information because of the broad market expectation that at least two interest rate increases were going to occur. We independently corroborated Chair Powell’s assertion through a review of the FOMC’s December 14, 2022, Summary of Economic Projections as well as media articles, which showed that there was a broad market expectation that at least two interest rate increases were going to occur. Although, as noted by (b) (6), (b) (7)(C), the chair’s statement gives the appearance of Class I FOMC information, section IV(D) of the *Program for Security of FOMC Information* authorizes the chair to make exceptions for the disclosure of confidential FOMC information. This policy section states, “The Chair may make ad-hoc exceptions to this section that are either more or less restrictive for particular documents or for other confidential information.” During our interview with (b) (6), (b) (7)(C) he explained that section IV(D) provides the chair with the authority to “up classify or down classify” FOMC information at any time.

Conclusion

In conclusion, we have found no violations of law, regulation, or policy associated with this matter. During the course of our review, we learned that IF staff wanted to meet with the chair to discuss process improvements, and, to date, no meeting or other communication has occurred. As a result, we referred these investigative findings to the OIG’s OIT. In light of our referral and as part of its 2023 audit of the Board’s information security program, required by the Federal Information Security Modernization Act of

³ Confidential FOMC information includes all privileged information that comes into the possession of the Board members, Federal Reserve Bank presidents, or Federal Reserve System staff in the performance of their duties for, or pursuant to the direction of, the committee. Such information covers, but is not limited to, expressions of policy views at committee meetings, reasons for those views, votes of the committee, and staff forecasts. The information that must be kept confidential may be in any form. It includes not only paper documents, but also electronic messages and files, recordings, notes, oral briefings, and discussions relating to confidential FOMC matters. Confidential FOMC information is divided into three classes: Class I, Class II, and Class III. Class I FOMC information generally applies to information that includes policymaker input, such as information related to monetary policy decisions at meetings, nonpublic views expressed by policymakers on likely future policy, and the identity of meeting participants who express particular views.

2014, OIT tested select security controls for (b) (7)(E) (b) (7)(E) [REDACTED]

[REDACTED] Based on the review, the Board has taken actions to strengthen security controls for (b) (7)(E) OIT plans to issue a restricted audit report detailing the results of its testing of (b) (7)(E) to include specific recommendations, by the end of 2023. As a result of these findings, no further investigation is required, and this investigation will be closed.

**Office of Inspector General**

Board of Governors of the Federal Reserve System
Consumer Financial Protection Bureau

MEMORANDUM

DATE: November 27, 2023

TO: Jeff Riedel
Chief Information Officer
Board of Governors of the Federal Reserve System

FROM: Khalid Hasan 
Assistant Inspector General for Information Technology

SUBJECT: OIG Report 2023-IT-B-018R: *Results of Security Control Testing of a Videoconferencing Platform Used by the Board*

Executive Summary

The Federal Information Security Modernization Act of 2014 (FISMA) requires offices of inspector general to evaluate the effectiveness of the information security controls and techniques for a subset of their agency's information systems. To meet FISMA requirements, we reviewed selected information security controls for a videoconferencing platform used by the Board of Governors of the Federal Reserve System. The Board promoted use of the platform for staff to collaborate with external parties during the COVID-19 pandemic and in the subsequent hybrid work environment.

Overall, the security controls we tested for the videoconferencing platform were effective. For example, the Board ensured that privileged access to the platform was provisioned on a need-to-know basis. However, we identified opportunities for improvement related to account management policies and procedures, audit log review, and security assessment and authorization processes. The Board took actions to address the findings related to account management and audit log review before the issuance of this memorandum report. As such, this memorandum report includes one matter for management consideration related to the Board's security assessment and authorization processes.

Given the sensitivity of the information in our review, our full memorandum report is restricted.

Background

FISMA requires agencies to develop, document, and implement an agencywide security program for the information and the information systems that support the operations and assets of the agency.¹ FISMA also requires inspectors general to perform an annual, independent evaluation to determine the effectiveness of the information security program and practices of their respective agency. The independent evaluation is to include testing the effectiveness of controls for a subset of the agency’s information systems. As part of our 2023 FISMA audit, we reviewed the effectiveness of selected information security controls for (b) (7)(E).²

(b) (7)(E)
. ³ In the first quarter of 2020, the Board began a period of extended full-time telework because of the COVID-19 pandemic and promoted the use of (b) (7)(E) to facilitate work with external parties. In April 2023, the Board implemented a significant change to (b) (7)(E) that (b) (7)(E).⁴ While the Board allows its employees to use multiple conferencing solutions depending on the needs of the meeting, the agency advises its employees to use (b) (7)(E) for any meetings involving users outside the Board or the Federal Reserve System.

Prior Work Performed by the OIG

On July 6, 2023, we issued a restricted, early alert memorandum to bring to Division of Information Technology management’s attention initial observations from our security control testing of the Board’s implementation of (b) (7)(E).⁵ We communicated these observations before the completion of our audit so that the Board could take steps to strengthen security controls and reduce the risk associated with the use of (b) (7)(E). The Board has taken several steps to address the observations we communicated, and as such, we are not issuing any recommendations (see table). We plan to follow up on the Board’s actions as part of future FISMA audits.

¹ Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (2014) (codified at 44 U.S.C. §§ 3551–3558).

² Office of Inspector General, *2023 Audit of the Board’s Information Security Program*, OIG Report 2023-IT-B-015, September 29, 2023.

³ The Board does not have all (b) (7)(E) collaboration features enabled.

⁴ (b) (7)(E)

⁵ Office of Inspector General, *OIG Early Alert Memorandum: Initial Observations on (b) (7)(E) Security Controls*, July 6, 2023.

Table. OIG Early Alert Memorandum Observations on (b) (7)(E) Security Controls and Actions Taken

Observation	Actions taken by the Board
The Division of IT did not (b) (7)(E) [redacted]	(b) (7)(E) [redacted]
The Division of IT had not (b) (7)(E) [redacted]	(b) (7)(E) [redacted]
The Division of IT had not ensured (b) (7)(E) [redacted]	(b) (7)(E) [redacted]
The Division of IT can strengthen (b) (7)(E) [redacted]	(b) (7)(E) [redacted]

Source: OIG analysis.

Objectives, Scope, and Methodology

The objectives of our 2023 FISMA audit were to evaluate the effectiveness of the Board’s (1) security controls and techniques for selected information systems and (2) information security policies, procedures, standards, and guidelines. To support our objectives, we assessed the effectiveness of selected security controls for three of the Board’s information systems, including (b) (7)(E).⁶ The scope of our (b) (7)(E) testing included 21 controls in 7 families from National Institute of Standards and Technology (NIST), Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (SP 800-53): access control; audit and accountability; assessment, authorization, and monitoring; contingency planning; planning; risk assessment; and system and information integrity. The controls were selected based on a risk assessment and their alignment to the Office of Management and

⁶ We selected these three systems using a risk-based approach that includes various factors, such as the system’s purpose, the information maintained within the system, and the function of the system.

Jeff Riedel

November 27, 2023

Budget’s fiscal year 2023–2024 FISMA reporting metrics for inspectors general.⁷ The attachment to this memorandum provides a listing of the 21 specific controls included in our scope that were determined to be applicable application-level controls.

To evaluate security controls for (b) (7)(E) we

- analyzed security policies, procedures, and documentation, including (b) (7)(E)
- interviewed Division of IT management and staff
- observed and tested specific (b) (7)(E) security processes and controls, including the administrative functions of the (b) (7)(E)
- reviewed (b) (7)(E) audit logs covering the (b) (7)(E) time frame

We performed this testing as part of our annual FISMA audit of the Board’s information security program, which is conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives.

Results

Overall, the security controls we tested for (b) (7)(E) were effective. For example, the Board ensured that privileged access to (b) (7)(E) was provisioned on a need-to-know basis. However, we identified opportunities for improvement related to account management policies and procedures, audit log review, and security assessment and authorization processes. The Board took action to address the findings related to account management and audit log review before the issuance of this memorandum report. As such, this memorandum report includes one item for management consideration related to the Board’s security assessment and authorization processes.

Finding 1: The (b) (7)(E) Account Management (b) (7)(E)

(b) (7)(E)
(b) (7)(E)
(b) (7)(E)

We found several issues related to the comprehensiveness of the (b) (7)(E). Specifically, we noted that (b) (7)(E). In addition, we found that the Board can ensure that the policy is fully implemented. We noted that the (b) (7)(E)

⁷ Office of Management and Budget, *FY 2023–2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, February 10, 2023.

The Board's (b) (7)(E) [redacted]
[redacted]
[redacted]

[redacted] In addition, NIST SP 800-53 requires that the information system owner specify the authorized users of the information system, group and role membership, and access authorizations (meaning, privileges) and other attributes, as required.

We believe these issues are attributable to the relatively small team managing (b) (7)(E) and their familiarity with the day-to-day operations of the system, (b) (7)(E) [redacted]
[redacted]
[redacted]
[redacted]

Management Actions Taken

(b) (7)(E) [redacted]
[redacted]
[redacted]
[redacted]

Finding 2: (b) (7)(E)

[redacted]
[redacted]
[redacted]

We found that the (b) (7)(E) team did not consistently (b) (7)(E) [redacted] in accordance with the Board's (b) (7)(E) [redacted] and (b) (7)(E) internal procedures. Specifically, while we found that (b) (7)(E) [redacted] were documented for the (b) (7)(E) [redacted], time frame, there were three instances in which (b) (7)(E) [redacted]. In addition, only (b) (7)(E) [redacted] were documented for the (b) (7)(E) [redacted], period.

The Board's (b) (7)(E) [redacted] states that owners of (b) (7)(E) systems are required to review (b) (7)(E) [redacted]. Further, the (b) (7)(E) procedures require the (b) (7)(E) team to perform a (b) (7)(E) [redacted] by running a report from the (b) (7)(E) [redacted] and documenting performance of the review. The manual nature of the (b) (7)(E) [redacted] [redacted]. Board officials assured us that the (b) (7)(E) [redacted] [redacted]. Performing and documenting a (b) (7)(E) [redacted] will provide the Board with assurance of its security posture as it relates to (b) (7)(E) and (b) (7)(E) [redacted].

Management Actions Taken

(b) (7)(E) [redacted]
[redacted]
[redacted]

Matter for Management Consideration: The Board’s Requirements Regarding Significant System Changes Can Be Clarified

In our July 6, 2023, early alert memorandum, we reported that (b) (7)(E) [redacted]

(b) (7)(E) [redacted]

In response to our (b) (7)(E) [redacted]. After this initial response, these officials were able to gather more details and informed us that the (b) (7)(E) [redacted] of (b) (7)(E) [redacted] included (b) (7)(E) [redacted] controls within its scope, anticipating the change from the (b) (7)(E) [redacted] to the (b) (7)(E) [redacted] application. (b) (7)(E) [redacted]

[redacted]. Further, Division of IT officials informed us they plan to revisit their policies in this area to (b) (7)(E) [redacted] and the resulting (b) (7)(E) [redacted]

Strengthening the requirements in this area will help ensure that the IS&P team is informed of (b) (7)(E) [redacted] and that the necessary security assessment and authorization activities occur (b) (7)(E) [redacted]. While we are not making a recommendation at this time, we plan to follow up on the Board’s actions in this area as part of our future FISMA audits.

Closing

Overall, the security controls we tested for (b) (7)(E) [redacted] were effective. However, we identified opportunities for improvement related to account management policies and procedures, audit log review, and security assessment and authorization processes. The Board took action to address the findings related to account management and audit log review before the issuance of this memorandum report. As such, this memorandum report includes one item for management consideration related to the Board’s security assessment and authorization processes. This memorandum is provided for information purposes. A formal response is not required.

⁸ Office of Inspector General, *OIG Early Alert Memorandum: Initial Observations on (b) (7)(E) Security Controls*, July 6, 2023.

Jeff Riedel

November 27, 2023

We appreciate the cooperation that we have received from your staff during our review. If you have any questions, please feel free to contact Paul Vaclavik, OIG manager, at 202-736-1928 or me at 202-973-5058.

Attachment

cc: Patrick J. McClanahan
Kofi Spong
Charles Young
William Dennison
Delwyn Lee
Sahir Zuberi
Dmitry Tomchuk
Annie Martin
Martha West
Adam Ndam

Attachment**Security Controls Tested for (b) (7)(E)**

Control no.	Control name
Access control	
AC-2	Account management
AC-2(3)	Account management—Disable accounts
AC-5	Separation of duties
AC-6	Least privilege
AC-6(9)	Least privilege—Log use of privileged functions
AC-8	System use notification
Audit and accountability	
AU-2	Audit events
AU-3	Content of audit records
AU-6	Audit review, analysis, and reporting
AU-11	Audit record retention
Assessment, authorization, and monitoring	
CA-2	Security assessments
CA-3	Information exchange
CA-5	Plan of action and milestones
CA-6	Security authorization

Jeff Riedel

November 27, 2023

Control no.	Control name
Contingency planning	
CP-2	Contingency plan
CP-4	Contingency plan testing
Planning	
PL-2	System security plan
PL-4	Rules of behavior
Risk assessment	
RA-3	Risk assessment
RA-5	Vulnerability monitoring and scanning
System and information integrity	
SI-2	Flaw remediation

Source: National Institute of Standards and Technology, Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*.

Note: Controls with parentheses indicate a control enhancement.