IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

UNITED STATES OF AMERICA	)	
	)	
v.	)	Criminal Action No. 1:23-cr-61-MN
	)	
ROBERT HUNTER BIDEN,	)	
	)	
Defendant.	)	

REPLY TO DEFEDANT'S RESPONSE TO MOTION TO ADMIT RULE 1006 SUMMARY CHART AND FIND ELECTRONIC EVIDENCE SELF-AUTHENTICATING PURSUANT TO RULE 902(14)

The United States, by and through undersigned counsel, respectfully submits this Reply in support of the government's motion (Doc. No. 120). In his Response, the defendant says he does not object to the authenticity of the trial evidence because it "reflect[s] what investigators collected and what existed at the time they obtained it." Doc. No. 151 at p. 1, FN 1. The government therefore respectfully requests that the Court enter its proposed order prior to trial so that the government can finalize its exhibits and not require the attendance of unnecessary witnesses.[1]

In the remainder of his Response, defense counsel demonstrates (1) they still do not understand the electronic evidence in this case that they received in discovery last fall, and (2) despite claiming they do, they actually have no evidence to give them "reasons to believe that data has been altered and compromised before investigators obtained the electronic material." Doc. No.

[1] Federal Rule of Evidence 902 was amended to "set[] forth a procedure by which parties can authenticate certain electronic evidence other than through the testimony of a foundation witness," and with the recognition that "the expense and inconvenience of producing an authenticating witness" for certain types of records and data "is often unnecessary." Fed. R. Evid. 902 advisory committee's note (2017). The Committee Notes on the Rules further state, "It is often the case that a party goes to the expense of producing an authentication witness, and then the adversary either stipulates authenticity before the witness is called or fails to challenge the authentication testimony once it is presented. The amendment provides a procedure under which the parties can determine in advance of trial whether a real challenge to authenticity will be made, and can then plan accordingly." *Id.*

151 at p. 1. None of what they claim in their Response is admissible in court, and the government objects to any line of questioning suggesting the trial evidence may have been manipulated because there is no foundation for such questions, they are also irrelevant, and even the inference posed by such a question risks confusing the jury.

First, it should be noted that the defendant's laptop and his iCloud data come from two separate and independent sources.

Apple, Inc. provided the government with files, including iCloud 03 and iCloud 04, as referenced in the summary chart. These files did not originate from his laptop. Instead, Apple iCloud 03 is a backup of the defendant's Apple iPad Pro and Apple iCloud 04 is a backup of the defendant's Apple iPhone XR. As shown in the 1006 summary chart, Doc. No. 158-2, the government is introducing messages from these two devices from April 2018 through January 2019. Not only are these two devices not the laptop, the evidence from these sources predates when the defendant dropped his laptop off at a computer store on April 12, 2019 in a state of disrepair. *See* Search Warrant Affidavit at ¶ 65, Case No. 19-30M. The defendant has not offered any conspiracy theory, much less any evidence, regarding how or why Apple, Inc. produced manipulated data for his iPhone and iPad.

Second, the data from the laptop that the government is utilizing is not only self-authenticating, but it will be introduced with corroborating evidence at trial. Data that is included in the 1006 summary chart is derived from the defendant's Apple iCloud account, as denoted in the source column, with two exceptions:

(1) Messages between the defendant and Witness 3, beginning in row 88 because the defendant began using his ex-wife's phone in October 2018 and her old phone was not synced to his iCloud account. Witness 3 will testify to the authenticity of these messages at trial.

(2) Messages in Row 85-86 (a message where the defendant says "I need more chore boy," which is used consistently in the message with how the defendant described "chore boy" in his book), Rows 87 and 135-137 (messages where the defendant says he in Delaware, which is consistent with his ATM withdrawal activity, location information on photographs on his phone, and his admissions in his book), Row 214 (a photograph of the defendant with a crack pipe in his hand), and 216-292 (videos and photographs of the defendant with a crack pipe and drug messages from December to March 2019, consistent with the defendant's characterization of his activity in his book).

What are the messages the defendant is claiming were somehow retroactively planted into his non-functional laptop, and what is the evidence of that? There is none. He has not shown any of the actual evidence in this case is unreliable or inauthentic, because there is none.

Instead, the defendant's theory about the laptop is a conspiracy theory with no supporting evidence. The defendant cites a book written by John Mac Isaac, but apparently there is nothing in the book where Mac Isaac says he "altered" or "compromised" data because no such passages are quoted in the defendant's response. The defendant is in a civil lawsuit with Mac Isaac and deposed him, but cites no evidence from that case or deposition to support his claims of alteration. The defendant next cites a *Washington Post* article and argues that a copy of data that Mac Isaac apparently provided to at least one third party in August of 2020 which was later obtained by the *Washington Post* reviewer was of poor forensic quality. But what the government is using in trial are actual extractions by an FBI forensic specialist which were extracted after a technical examination of the laptop in 2019, not whatever files were supposedly released by Mac Isaac in August 2020 and were eventually obtained by the *Washington Post* after who-knows-what was added to them by third parties that have nothing to do with this criminal case. The defendant also relies on an allegation that a Russian businessman told a third-party that Biden's devices were

compromised by FSB during his 2014 trip to Kazakhstan. This is yet another example of the defendant asking people to believe Russian intelligence when it suits his interests, but not to believe Russian intelligence when it doesn't suit his interests. None of this hearsay on hearsay is evidence, and none of it demonstrates that the actual trial evidence was altered. Any questioning suggesting this would be without a foundation.

The lack of any basis for his claims is further underscored by the fact that the defendant has indicated he has no reciprocal discovery. The defendant has had the laptop data in its raw, original form since September 2023, but has provided the government with no evidence of its manipulation or alteration. He has not provided any evidence or information that shows that his laptop contains false information, and the government's evidence shows the opposite – the defendant's laptop is real (it will be introduced as a trial exhibit) and it contains significant evidence of the defendant's guilt (see 1006 summary chart). Moreover, the evidence on his laptop is corroborated by independent sources including witnesses, like Witness 3 who will confirm the authenticity of the messages. It is also corroborated by the defendant's own admissions in his book which are consistent with the evidence on the laptop, photographs and videos of the defendant himself, and evidence obtained from third parties, such as his bank statements and Apple, Inc., which match information on his laptop. Any argument that suggests his laptop is not authentic would be inappropriate because there is no foundation for such questioning, and it risks creating juror confusion about the evidence actually at issue in this case.

The government requests that the Court grant the motion because the records are self-authenticating. The government further requests that the Court prohibit the defendant from suggesting that the electronic evidence is fabricated, manipulated, altered, or inauthentic because he has not offered any evidence supporting such a claim.

Respectfully submitted,

DAVID C. WEISS
Special Counsel
United States Department of Justice

By: 

Derek E. Hines
Senior Assistant Special Counsel
Leo J. Wise
Principal Senior Assistant Special Counsel
United States Department of Justice
950 Pennsylvania Avenue NW
Washington, D.C. 20530
771-217-6091

Dated: May 22, 2024