

STANLEY A. TWARDY, JR.  
Attorney at Law

One Canterbury Green  
Stamford, CT 06901-2047  
T: (203) 977-7368 F: (866) 458-1037  
satwardy@daypitney.com

July 25, 2016

**VIA UPS**

The Honorable Ron Johnson  
Chairman  
Committee on Homeland Security & Governmental Affairs  
United States Senate  
328 Hart Senate Office Building  
Washington, D.C. 20510

The Honorable Lamar Smith  
Chairman  
Committee on Science, Space and Technology  
United States House of Representatives  
2321 Rayburn House Office Building  
Washington, D.C. 20515

Dear Chairmen Johnson and Smith:

We represent Datto, Inc., (“Datto”) and write in response to your letter to Datto Chief Executive Officer Austin McChord dated July 12, 2016, in which you “reiterate [your] previous requests for information,” referencing Chairman Johnson’s letter of October 5, 2016 and Chairman Smith’s letter of January 14, 2016.

By letters dated October 19, 2015 and January 27, 2016<sup>1</sup> I responded, on Datto’s behalf, to both letters. In those responses we provided extensive information responding to the inquiries. However, with respect to some inquires we advised that we were unable to comply due to “Datto’s data privacy policies and its contractual confidentiality requirements.” Upon receipt of your July 12, 2016 letter, we notified Datto’s client, Platte River Networks (“Platte River”) of your renewed inquiry, and asked them to advise whether they continued to object to disclosure of “Confidential Information” as described in my earlier responses to you. We have been informed that Platte River continues to object to disclosure. Accordingly, Datto cannot

---

<sup>1</sup> The January 27, 2016 letter was erroneously dated January 27, 2015. Both letters are enclosed.



The Honorable Ron Johnson  
The Honorable Lamar Smith  
July 25, 2016  
Page 2

disclose any such Confidential Information unless required by law or by order of a court or governmental agency.

Please do not hesitate to contact me, or my colleague Steven Cash (202-218-3912), who is resident in our Washington, D.C. office, if you have any questions.

Very truly yours,

A handwritten signature in black ink that reads 'Stanley A. Twardy, Jr.' with a large, stylized flourish at the end.

Stanley A. Twardy, Jr.

SAT/ms  
Enclosures



The Honorable Ron Johnson  
The Honorable Lamar Smith  
July 25, 2016  
Page 3

cc: The Honorable Thomas R. Carper  
Ranking Member  
Committee on Homeland Security & Governmental Affairs  
United States Senate  
513 Hart Senate Office Building  
Washington, D.C. 20510

The Honorable Eddie Bernice Johnson  
Ranking Member  
Committee on Science, Space and Technology  
United States House of Representatives  
2321 Rayburn House Office Building  
Washington, D.C. 20515

David Brewer, Esq.  
Chief Counsel for Oversight and Investigations  
Committee on Homeland Security & Governmental Affairs  
United States Senate  
Washington, D.C. 20510  
*Via E-Mail Only, David\_Brewer@hsgac.senate.gov*

James Secreto, Esq.  
Chief Counsel for Oversight and Investigations (Minority)  
Committee on Homeland Security & Governmental Affairs  
United States Senate  
Washington, D.C. 20510  
*Via E-Mail Only, Jim\_Secreto@hsgac.senate.gov*

Ashley H. Callen, Esq.  
Staff Director & Chief Counsel for Investigations  
Oversight Subcommittee  
Committee on Science, Space and Technology  
2321 Rayburn HOB  
Washington, D.C. 20515  
*Via E-Mail Only, Ashley.Callen@mail.house.gov*

Mr. Jonathan McGee  
Legislative Assistant  
Office of Congresswoman Edie Bernice Johnson  
2468 Rayburn Office Building  
Washington, DC 20515  
*Via E-Mail Only, jonathan.mcgee@mail.house.gov*

STANLEY A. TWARDY, JR.  
Attorney at Law

One Canterbury Green  
Stamford, CT 06901-2047  
T: (203) 977-7368 F: (866) 458-1037  
satwardy@daypitney.com

October 19, 2015

VIA UPS

The Honorable Ron Johnson  
Chairman  
Committee on Homeland Security & Governmental Affairs  
United States Senate  
Washington, D.C., 20510

The Honorable Thomas R. Carper  
Ranking Member  
Committee on Homeland Security & Governmental Affairs  
United States Senate  
Washington, D.C., 20510

Dear Chairman Johnson and Ranking Member Carper:

We represent Datto, Inc., (“Datto”) and write further to our October 7, 2015 letter in response to Chairman Johnson’s letter to Datto Chief Executive Officer Mr. Austin McChord dated October 5, 2015.

In your October 5<sup>th</sup> letter, you requested that Datto voluntarily provide certain information to assist the Committee to “better understand Datto’s role relating to Secretary Clinton’s private server, the backup and security capabilities of the private server, and any directives provided to Datto relating to the server.”<sup>1</sup> This letter responds to those requests and reiterates Datto’s intention to continue responding to and complying with the requests in your letter, to the extent permitted by Datto’s data privacy policies and its contractual confidentiality requirements.

---

<sup>1</sup> Letter from The Honorable Ron Johnson to Mr. Austin McChord, dated October 5, 2015, at p. 4. It is our understanding that your request contemplates a voluntary response, and that no subpoena has issued pursuant to the *Rules of Procedure of the Committee on Homeland Security and Governmental Affairs*, March 2015.

The Honorable Ron Johnson  
The Honorable Thomas R. Carper  
October 19, 2015  
Page 2

The relevant terms of those requirements as stated in a typical Reseller Agreement include:

“Confidential Information” means any information, whether oral, written, electronic, or in any other format, and whether technical or business in nature, regarding this Agreement, Datto’s products or business, including the Product, information regarding a party’s products, services, Marks, software, intellectual property, equipment, pricing, marketing and business plans, other information not generally known to the public and any other information received under circumstances reasonably interpreted as imposing an obligation of confidentiality; provided that, “Confidential Information” shall not include any of such information which: (i) was publicly available at the time of disclosure by the disclosing party; (ii) became publicly available after disclosure through no fault of the receiving party; (iii) was known to the receiving party prior to disclosure by the disclosing party; or (iv) was rightfully acquired by the receiving party after disclosure by the disclosing party from a third party who was lawfully in possession of the information and was under no legal duty to the disclosing party to maintain the confidentiality of the information.

*Required Disclosures.* Either party may disclose Confidential Information to the extent disclosure is based on the good faith written opinion of such party’s legal counsel that disclosure is required by law or by order of a court or governmental agency; provided that, the party that is the recipient of such Confidential Information shall use all commercially reasonable efforts to maintain the confidentiality of the Confidential Information by means of a protective order or other similar protection and shall give the owner of such Confidential Information prompt notice in order that it have every opportunity to intercede in such process to contest such disclosure and shall use all commercially reasonable efforts to cooperate with the owner of such Confidential Information to protect the confidentiality of such Confidential Information. The owner of such Confidential Information reserves the right to obtain a protective order or otherwise protect the confidentiality of such Confidential Information.

On October 6, 2015, in accordance with its obligations under the Reseller Agreement, Datto notified Platte River Networks (“Platte River”) of your October 5 inquiry, and asked whether they would object to disclosure of the information and materials requested. Platte River advised us that they had “no objection.” However, on October 14, 2015, counsel to Platte River withdrew their previous non-objection, and objected to any further disclosure of Confidential Information (as defined in the Reseller Agreement) to the Committee. Accordingly, Datto cannot disclose any such Confidential Information unless required by law or by order of a court or governmental agency.

The Honorable Ron Johnson  
The Honorable Thomas R. Carper  
October 19, 2015  
Page 3

Our review of documents and other materials related to your requests continue, and should that effort reveal additional information responsive to your requests that is not confidential, we will supplement this response.

## I. BACKGROUND

Datto is a back-end service provider to thousands of managed IT service providers – often referred to as Managed Service Providers (“MSPs”) or “Resellers” such as Platte River. MSPs are often sophisticated, professional companies that provide a defined set of IT operations and services to their clients or “End-Users.” Datto works almost exclusively with these MSPs to provide comprehensive and secure “hybrid cloud” backup, data recovery, and business continuity solutions that the MSPs in turn resell and administer to End-Users. To accomplish this, Datto provides hardware, software and technical services to MSPs, as more fully described below. Datto also provides MSP customers with training on how to use Datto services.

Datto’s services to MSPs are generally governed by Reseller Agreements between the MSP and Datto. These contracts contain mutual and binding confidentiality clauses. As previously discussed, such a clause applies in Datto’s contract with Platte River. Rarely does Datto deal directly with an End-User, and in the matter referred to in your inquiry, Datto’s contractual relationship was with Platte River only. Datto was not aware of the identity of the End-User until reading allegations in the media.

Datto’s hybrid cloud solution involves two parts: (i) a local hardware backup device, such as the Datto SIRIS device (a “Local Device”); and (ii) a replicated offsite backup.<sup>2</sup> First, the Datto solution uses software to take a full backup image of the End-User’s IT environment that is being backed up (servers, data, etc.) and copies it onto a Local Device, which is a hardware device that is often located in the same physical location as the IT environment it is backing up (i.e. the “server room”). From there, the Local Device works as a “failover” system in the event of a business interruption that impacts the End-User’s IT environment. Second, a duplicate copy of all of the information stored on the Local Device is also placed on a replicated storage device (a “Storage Node”) that is located at a different location (i.e. “offsite”) than the Local Device.<sup>3</sup> Offsite replication ensures that if the event that caused the End-User’s system to fail also impacts the Local Device (e.g. a fire or flood) the MSP can use the cloud – “Datto Cloud” or a “Private Cloud” – as an alternative failover system from the Local Device.

In most use cases, the MSP chooses for offsite replication to occur at a Datto-controlled data center facility. Datto refers to this approach as a “Datto Cloud” solution. In other use cases,

---

<sup>2</sup> In this letter “local” refers to the physical location of the MSP’s systems.

<sup>3</sup> This duplication is accomplished by the creation of multiple restore points that can be individually reconstructed to restore the dataset as it previously existed at a particular time.

The Honorable Ron Johnson  
The Honorable Thomas R. Carper  
October 19, 2015  
Page 4

MSPs may choose to replicate backed-up data offsite to a Storage Node owned and operated by the MSP at a site of its choosing. Datto refers to this approach as a “Private Cloud.”

As an alternative to a hybrid cloud approach, an MSP may opt out of offsite replication altogether and request a “Local Only” setup. In a Local Only configuration, backed-up data will not replicate beyond the Local Device. Because Datto’s technology solution is meant to be deployed as a hybrid cloud solution, to set up a Local Only solution, generally the MSP must work directly with Datto technical support to implement this. By default, absent a functioning private offsite Storage Node or the requisite communications with Datto technical support, all Local Devices replicate to the Datto Cloud.

As noted, as a back-end service provider, Datto very rarely—if ever—has any direct interaction with the End-Users served by the MSPs. The nature of Datto’s relationship with MSPs precludes Datto from knowing either the identity of End-Users and the content of the data stored on the Local Device or replicated offsite. Datto has no role in monitoring the content or source of data stored by MSP clients such as Platte River. As such, Datto would not be aware of who was Platte River’s End-User and Datto did not and does not have any knowledge concerning the content of any data that may or may not have been backed up to the Datto Cloud, or stored on the Datto SIRIS device owned and operated by Platte River.<sup>4</sup>

## II. DATTO INVOLVEMENT IN MATTERS RELATED TO THE COMMITTEE’S INQUIRY

Datto first became aware that Platte River had been contacted by U.S. Government officials inquiring into Platte River’s involvement with former Secretary Clinton’s e-mail server through media reports on or about Sunday, August 9, 2015. Soon thereafter, Datto disconnected the replicated offsite Storage Node, and independently took prudential steps to preserve information within Datto’s control which Datto believed could be subject to law enforcement or other governmental inquiry.

On September 10, 2015, Datto received a *Request for Preservation of Records* from the Federal Bureau of Investigation (FBI) requesting that Datto preserve records related to a Datto Local Device identified by the FBI. Datto informed the FBI on September 16, 2015 that Datto had disconnected and preserved an offsite Storage Node associated with the Local Device. On October 6, 2015, with the consent of Platte River and its End-User, Datto provided the Storage Node to the FBI. The FBI has custody of the Storage Node.

---

<sup>4</sup> Datto’s standard contracts permit communication with an End-User, but this rarely is done, and was not in this case. In rare cases, Datto will be asked to directly assist an End-User.

The Honorable Ron Johnson  
The Honorable Thomas R. Carper  
October 19, 2015  
Page 5

III. RESPONSES TO INFORMATION REQUESTS

Please note that with respect to questions 1-4, 7, 8 and 9, these requests call for the production of documents and materials that are Confidential Information as defined by the Datto Reseller Agreement and Datto's data privacy policies. Consequently, Datto is not authorized to disclose such information absent consent from its client, Platte River, or unless required by law or by order of court or governmental agency.

With respect to questions to which the immediately preceding paragraph does not apply, Datto responds as follows:

5. *Is Datto authorized to store classified information? Were any Datto employees authorized to view classified information? Please explain. Did Datto's contract regarding Secretary Clinton's private server include provisions related to the storing of classified information?*

**RESPONSE:** Datto is not authorized to store classified information, and does not offer storage of classified information as part of its business.<sup>5</sup> No Datto employees are authorized to access classified information in the context of their employment at Datto. Datto has never entered into any contracts containing provisions related to the storage of classified information.

6. *Has Datto been contacted by the Federal Bureau of Investigation (FBI) or any other law-enforcement entity regard (sic) Secretary Clinton's private server? Has Datto turned over any information, materials, or equipment to the FBI or any other law enforcement entity? Please explain.*

**RESPONSE:** On September 10, 2015, Datto received a *Request for Preservation of Records* from the FBI, requesting that Datto preserve records related to a Datto Local Device identified by the FBI. Datto informed the FBI on September 16, 2015 that Datto had disconnected and preserved an offsite Storage Node associated with the Local Device. On October 6, 2015, with the consent of Platte River and its End-User, Datto provided the Storage Node to the FBI. The FBI has custody of the Storage Node.

8. *Please explain the process for storing data in the Datto Cloud.*  
*a. How long is data retained in the cloud?*  
*b. What happens to the data once the required retention period is reached?*

---

<sup>5</sup> For purposes of this response "classified information" means information classified pursuant to Executive Order 13526. Datto does not hold a Facilities Clearance (FCL) as administered by the Defense Security Service, or any other U.S. Government agency or department.

The Honorable Ron Johnson  
The Honorable Thomas R. Carper  
October 19, 2015  
Page 6

- c. *Is the data deleted automatically?*
- d. *As mentioned above, CESC requested that the retention period for backups be reduced to 30 days. What information would be lost by reducing the backup retention period to 30 days? Please explain.*

**RESPONSE:** To the extent Chairman Johnson's request calls for a general outline of the process for storing data in the Datto Cloud, or Datto's security capabilities and functions, we note that Datto's security efforts include hardware, software, and encryption mechanisms as well as physical, technical and administrative controls. The details of these capabilities are confidential, and public disclosure of those details could reveal vulnerabilities and capabilities of Datto's systems, infrastructures, projects, plans, or protection services relating to its business and the data entrusted to Datto by its MSP customers. As such, public disclosure of these capabilities could cause Datto's systems to become less secure.

The Datto Cloud has over 140 petabytes of cloud storage capacity. Usage of that storage capacity fluctuates depending on the retention settings established by the MSP. That said, Datto's solution takes an exact and comprehensive backup image of the entire host machine that it backs up. The Datto solution will keep an image of everything that was on the host machine when the last backup was taken. Users generally take that image every day, usually more than once per day. The data is stored in a snapshot capable file system that tracks the state of the backups back in time. At any one point, the solution will have the most recent copy of the machine it backs up as well as a number of exact copies of prior versions depending on the retention settings that the MSP has chosen. If the retention settings are 30 days, that means that the picture the Datto Solution takes on day 1 will roll off the backup chain on day 31.

The following is an example of how a specific retention setting would apply to a theoretical unit of data. This example assumes a 30 day retention setting, and that user settings provide for only one full backup per day.

Day 1 – The backup includes a word document (“Document A”) that is sitting on the host machine.

Day 15 – Before the day's backup was taken, the user makes changes to Document A. Rather than saving the changes to a new word document, the user just writes over Document A.

Day 30 – The user realizes that she liked the way Document A was drafted before she wrote over it. The Datto solution took an image of Document A on each of days 1 through 14 (before it was written over). The user can retrieve that Document A from the backup images made on days 1 through 14.

The Honorable Ron Johnson  
The Honorable Thomas R. Carper  
October 19, 2015  
Page 7

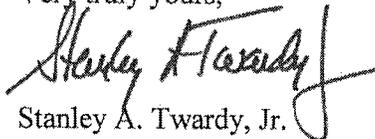
Day 60 – Assume that the user did not realize until day 60 that she liked the way Document A was drafted before she changed it. Document A is no longer recoverable because the last backup of that document would have dropped off the backup chain on day 44.

That said, an image based backup is a sparse file. It is a block by block copy of the host machine that it backs up. When data is removed from the file system, in most cases the file system does not automatically “zero out” the de-referenced blocks on a hard drive. Rather, a metadata store marks those blocks as free for future use. So, there remains a potential that de-referenced blocks of data may still reside on a hard drive.

#### IV. CONCLUSION

Thank you for the opportunity to assist the Committee in its work. Please do not hesitate to contact me if you have any questions.

Very truly yours,



Stanley A. Twardy, Jr.

cc: Michael Joseph Lueptow  
Investigative Counsel  
Committee on Homeland Security & Governmental Affairs  
United States Senate  
Washington, D.C., 20510  
*Via E-mail*

Scott D. Wittmann  
Investigative Counsel  
Committee on Homeland Security & Governmental Affairs  
United States Senate  
Washington, D.C., 20510  
*Via E-mail*

James Secreto  
Chief Counsel for Oversight and Investigations (Minority)  
Committee on Homeland Security & Governmental Affairs  
United States Senate  
Washington, D.C., 20510  
*Via E-mail*

STANLEY A. TWARDY, JR.  
Attorney at Law

One Canterbury Green  
Stamford, CT 06901-2047  
T: (203) 977-7368 F: (866) 458-1037  
satwardy@daypitney.com

January 27, 2015

**VIA UPS**

The Honorable Lamar Smith  
Chairman  
Committee on Science, Space and Technology  
United States House of Representatives  
2321 Rayburn House Office Building  
Washington, D.C. 20515

The Honorable Eddie Bernice Johnson  
Ranking Member  
Committee on Science, Space and Technology  
United States House of Representatives  
2321 Rayburn House Office Building  
Washington, D.C. 20515

Dear Chairman Smith and Ranking Member Johnson:

We represent Datto, Inc., (“Datto”) and write further to our January 15, 2016 letter in response to Chairman Smith’s letter to Datto Chief Executive Officer Austin McChord dated January 14, 2016.

In your January 14 letter, the Committee requested Datto’s “assistance in improving the National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity (the Framework) and the Federal Information Security Act (*sic*) (FISMA).”<sup>1</sup> The Committee also requested “documents and information relating to work your company performed for a former government official,” identified later in the letter as former

---

<sup>1</sup> We assume the reference is to the Federal Information Security Management Act of 2002, Pub. L. No. 107-296 tit. X, 116 Stat. 2259 (codified primarily at 44 U.S.C. §§ 3531-3538) and Federal Information Security Management Act of 2002, Pub. L. No. 107-347 tit. III, 116 Stat. 2946 (codified primarily at 44 U.S.C. §§ 3541-3549) repealed and replaced by Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (codified primarily at 44 U.S.C. §§ 3551-3558).

The Honorable Lamar Smith  
The Honorable Eddie Bernice Johnson  
January 27, 2016  
Page 2

Secretary of State Hillary Clinton.<sup>2</sup> As you know, a similar request was made of Datto by Chairman Ron Johnson of the U.S. Senate's Homeland Security and Government Affairs Committee.<sup>3</sup> As we explained in our reply<sup>4</sup> to Chairman Johnson's letter and as we reiterate here, Datto's response to such requests for information is governed by Datto's data privacy policies and its contractual confidentiality requirements.

The relevant terms of those requirements as stated in a typical Datto Reseller Agreement include:

"Confidential Information" means any information, whether oral, written, electronic, or in any other format, and whether technical or business in nature, regarding this Agreement, Datto's products or business, including the Product, information regarding a party's products, services, Marks, software, intellectual property, equipment, pricing, marketing and business plans, other information not generally known to the public and any other information received under circumstances reasonably interpreted as imposing an obligation of confidentiality; provided that, "Confidential Information" shall not include any of such information which: (i) was publicly available at the time of disclosure by the disclosing party; (ii) became publicly available after disclosure through no fault of the receiving party; (iii) was known to the receiving party prior to disclosure by the disclosing party; or (iv) was rightfully acquired by the receiving party after disclosure by the disclosing party from a third party who was lawfully in possession of the information and was under no legal duty to the disclosing party to maintain the confidentiality of the information.

*Required Disclosures.* Either party may disclose Confidential Information to the extent disclosure is based on the good faith written opinion of such party's legal counsel that disclosure is required by law or by order of a court or governmental agency; provided that, the party that is the recipient of such Confidential Information shall use all commercially reasonable efforts to maintain the confidentiality of the Confidential Information by means of a protective order or

---

<sup>2</sup> Letter from The Honorable Lamar Smith to Mr. Austin McChord, dated January 14, 2016. It is our understanding that your request contemplates a voluntary response, and that no subpoena has issued pursuant to the *Rules Governing Procedure, Committee on Science, Space and Technology, U.S. House of Representatives, 112th Congress*, available on-line at <https://science.house.gov/sites/republicans.science.house.gov/files/rules.pdf> (last visited Jan. 22, 2016).

<sup>3</sup> Letter from The Honorable Ron Johnson to Mr. Austin McChord, dated October 5, 2015 and attached hereto as Exhibit A.

<sup>4</sup> Letter from Stanley A. Twardy, Jr., Esq., to the Honorable Ron Johnson, dated October 19, 2015 and attached hereto as Exhibit B.

The Honorable Lamar Smith  
The Honorable Eddie Bernice Johnson  
January 27, 2016  
Page 3

other similar protection and shall give the owner of such Confidential Information prompt notice in order that it have every opportunity to intercede in such process to contest such disclosure and shall use all commercially reasonable efforts to cooperate with the owner of such Confidential Information to protect the confidentiality of such Confidential Information. The owner of such Confidential Information reserves the right to obtain a protective order or otherwise protect the confidentiality of such Confidential Information.

Despite misconceptions in the media, Datto's client in this matter was, and has always been, Platte River Networks ("Platte River"). On January 15, 2016, in accordance with its obligations under the Reseller Agreement, Datto notified Platte River of your January 14, 2016 inquiry, and asked whether they would object to disclosure of the information and materials requested. Counsel for Platte River responded on January 16, 2016, advising that Platte River "does object to disclosure of [the] 'information and materials requested.'" Accordingly, Datto cannot disclose any such Confidential Information absent consent from its client or unless required by law or by order of a court or governmental authority.

#### I. BACKGROUND

Datto is a back-end service provider to thousands of managed IT service providers – often referred to as Managed Service Providers ("MSPs") or "Resellers" such as Platte River. MSPs are often sophisticated, professional companies that provide a defined set of IT operations and services to their clients or "End-Users." Datto works almost exclusively with these MSPs to provide comprehensive and secure "hybrid cloud" backup, data recovery, and business continuity solutions that the MSPs in turn resell and administer to End-Users. To accomplish this, Datto provides hardware, software, cloud and technical services to MSPs, as more fully described below. Datto also provides MSP customers with training on how to use Datto services.

Datto's services to MSPs are generally governed by Reseller Agreements between the MSP and Datto. These contracts contain mutual and binding confidentiality clauses. As previously discussed, such a clause applies in Datto's contract with Platte River. Rarely does Datto deal directly with an End-User, and in the matter referred to in your inquiry, Datto's contractual relationship was with Platte River only. Datto was not aware of the identity of the End-User until reading allegations in the media in August of 2015.

Datto's hybrid cloud solution involves two parts: (i) a local hardware backup device, such as the Datto SIRIS device (a "Local Device"); and (ii) a replicated offsite backup.<sup>5</sup> First, the Datto solution enables the MSP to take a full backup image of the End-User's IT environment that is being backed up (servers, data, etc.) and copy it onto a Local Device, which is a hardware

---

<sup>5</sup> In this letter "local" refers to the physical location of the MSP's (or applicable End-User's) systems.

The Honorable Lamar Smith  
The Honorable Eddie Bernice Johnson  
January 27, 2016  
Page 4

device that is often located in the same physical location as the IT environment it is backing up (i.e. the “server room”). From there, the Local Device works as a “failover” system in the event of a business interruption that impacts the End-User’s IT environment. Second, a duplicate copy of all of the information stored on the Local Device is also placed on a replicated storage device (a “Storage Node”) that is located at a different location (i.e. “offsite”) than the Local Device.<sup>6</sup> Offsite replication ensures that if the event that caused the End-User’s system to fail also impacts the Local Device (e.g. a fire or flood) the MSP can use the cloud – “Datto Cloud” or a “Private Cloud” – as an alternative failover system from the Local Device.

In most use cases, the MSP chooses for offsite replication to occur at a Datto-controlled data center facility. Datto refers to this approach as a “Datto Cloud” solution. In other use cases, MSPs may choose to replicate backed-up data offsite to a Storage Node owned and operated by the MSP at a site of its choosing. Datto refers to this approach as a “Private Cloud.”

As an alternative to a hybrid cloud approach, an MSP may opt out of offsite replication altogether and request a “Local Only” setup. In a Local Only configuration, backed-up data will not replicate beyond the Local Device. Because Datto’s technology solution is meant to be deployed as a hybrid cloud solution, to set up a Local Only solution, generally the MSP must work directly with Datto technical support to implement this. By default, absent a functioning private offsite Storage Node or the requisite communications with Datto technical support, all Local Devices replicate to the Datto Cloud.

As noted, as a back-end service provider, Datto very rarely—if ever—has any direct interaction with the End-Users served by the MSPs. The nature of Datto’s relationship with MSPs precludes Datto from knowing either the identity of End-Users or the content of the data stored on the Local Device or replicated offsite. Datto has no role in monitoring the content or source of data stored by MSP clients such as Platte River. As such, Datto would not be aware of who was Platte River’s End-User and Datto did not and does not have any knowledge concerning the content of any data that may or may not have been backed up to the Datto Cloud, or stored on the Datto SIRIS device owned and operated by Platte River.<sup>7</sup>

## II. DATTO INVOLVEMENT IN MATTERS RELATED TO THE COMMITTEE’S INQUIRY

Datto first became aware that Platte River had been contacted by U.S. Government officials inquiring into Platte River’s involvement with former Secretary Clinton’s e-mail server through media reports on or about Sunday, August 9, 2015. Soon thereafter, Datto disconnected the replicated offsite Storage Node, and independently took prudential steps to preserve

---

<sup>6</sup> This duplication is accomplished by the creation of multiple restore points that can be individually reconstructed to restore the dataset as it previously existed at a particular time.

<sup>7</sup> Datto’s standard contracts permit communication with an End-User, but this rarely is done, and was not in this case. In rare cases, Datto will be asked to directly assist an End-User.

The Honorable Lamar Smith  
The Honorable Eddie Bernice Johnson  
January 27, 2016  
Page 5

information within Datto's control which Datto believed could be subject to law enforcement or other governmental inquiry.

On September 10, 2015, Datto received a *Request for Preservation of Records* from the Federal Bureau of Investigation (FBI) requesting that Datto preserve records related to a Datto Local Device identified by the FBI. Datto informed the FBI on September 16, 2015 that Datto had disconnected and preserved an offsite Storage Node associated with the Local Device. On October 6, 2015, with the consent of Platte River and its End-User, Datto provided the Storage Node to the FBI. It is our understanding that the FBI has custody of the Storage Node.

### III. RESPONSES TO DOCUMENT REQUESTS

Please note that with respect to Document Requests 1, 2 and 3, these requests call for the production of documents and materials that are Confidential Information as defined by the Datto Reseller Agreement and Datto's data privacy policies. Consequently, Datto is not authorized to disclose such information absent consent from its client, Platte River, or unless required by law or by order of court or governmental agency. As described above, Platte River has refused consent.

With respect to Question 4 ("All documents and communications referring or relating to the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity"), to the extent to which the immediately preceding paragraph does not apply, Datto responds as follows.

The National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity ("Framework")<sup>8</sup> is a voluntary framework developed to carry out President Obama's Executive Order<sup>9</sup> directing the "development of a voluntary Cybersecurity Framework ... that provides a 'prioritized, flexible, repeatable, performance-based, and cost-effective approach' to manage cybersecurity risk for those processes, information, and systems directly involved in the delivery of critical infrastructure services."<sup>10</sup> The Executive Order defines "critical infrastructure" as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

---

<sup>8</sup> *Nat'l Inst. of Standards & Tech., Framework for Improving Critical Infrastructure Cybersecurity*, Feb. 12, 2014.

<sup>9</sup> *Exec. Order No. 13636, Improving Critical Infrastructure Cybersecurity, DCPD-201300091*, Feb. 12, 2013.

<sup>10</sup> *Nat'l Inst. of Standards & Tech., Framework for Improving Critical Infrastructure Cybersecurity*, Feb. 12, 2014.

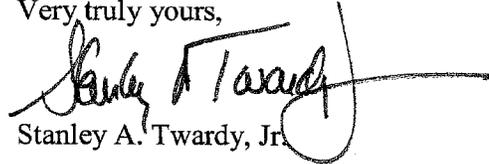
The Honorable Lamar Smith  
The Honorable Eddie Bernice Johnson  
January 27, 2016  
Page 6

Datto provides its backup and data recovery solutions to thousands of MSPs serving mostly small to medium sized businesses. Datto is committed to providing all of its clients with secure, reliable, and up-to-date solutions. The Framework, along with a host of other federal, industry and academic guidelines and standards offered by organizations such as the Information Systems Audit and Control Association, Payment Card Industry and the International Standards Organization, is well known to Datto, and is a valuable tool used throughout the IT industry, including Datto, as a reference document to guide internal security controls. As is clear from the Framework itself, however, it is not designed to be a contractual document or regulatory requirement, and it is not a part of Datto's contractual documentation or agreement with any of its clients.

#### IV. CONCLUSION

Thank you for the opportunity to assist the Committee in its work. Please do not hesitate to contact me if you have any questions.

Very truly yours,



Stanley A. Twardy, Jr.

cc: Drew Colliatie  
Caroline Ingram  
Professional Staff Members  
Committee on Science, Space and Technology, (Majority)  
United States House of Representatives  
2321 Rayburn House Office Building  
Washington, D.C., 20515  
*Via E-mail*

Jonathan McGee  
Legislative Assistant  
Committee on Science, Space and Technology, (Minority)  
United States House of Representatives  
2321 Rayburn House Office Building  
Washington, D.C., 20515  
*Via E-mail*

**EXHIBIT A**

RON JOHNSON, WISCONSIN, CHAIRMAN

JOHN MCCAIN, ARIZONA	THOMAS R. CARPER, DELAWARE
ROE PORTMAN, OHIO	CLAIRE McCASKILL, MISSOURI
RAND PAUL, KENTUCKY	JOE TESTER, MONTANA
JAMES LANKFORD, OKLAHOMA	TAMMY BALDWIN, WISCONSIN
MICHAEL B. ENZI, WYOMING	HEIDI HEITKAMP, NORTH DAKOTA
KELLY AYOTTE, NEW HAMPSHIRE	CORY A. BOOKER, NEW JERSEY
JONI ERNST, IOWA	GARY C. PETERS, MICHIGAN
BEN SASSE, NEBRASKA	

KEITH S. ASHDOWN, STAFF DIRECTOR  
GABRIEL F. A. BATKIN, MINORITY STAFF DIRECTOR

**United States Senate**  
COMMITTEE ON  
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS  
WASHINGTON, DC 20510-6250

October 5, 2015

Mr. Austin McChord  
Chief Executive Officer  
Datto, Inc.  
101 Merritt 7, 7th Floor  
Norwalk, CT 06851

Dear Mr. McChord:

The Committee on Homeland Security and Governmental Affairs is examining former Secretary of State Hillary Clinton's use of a private email account and server during her time at the State Department. The Committee has learned that a product offered by Datto, Inc.—the Datto SIRIS S2000<sup>1</sup>—was purchased in 2013 for Secretary Clinton to provide on-site, immediate recovery of backup data in the event that the primary server failed.<sup>2</sup> The Committee is interested in the security and preservation of Secretary Clinton's official records, including whether this backup device was used to back up, recover, or store those records in any manner. I request your assistance with this important inquiry.

Datto, Inc. is “an innovative provider of comprehensive backup, recovery and business continuity solutions used by thousands of managed service providers worldwide,” offering cloud, hardware, and software devices.<sup>3</sup> A Datto SIRIS device, like the one acquired for Secretary Clinton, “takes data directly from the server and converts it into virtual machines that can be booted instantly from a remote web interface.”<sup>4</sup> Essentially, if the primary server fails, the Datto device acts as a virtual server to allow continued workflow while the primary server is fixed.<sup>5</sup> When acquiring a Datto SIRIS device, Datto offers its clients two options for storing the virtualized backups. The first option is to store the backups on-site on the Datto SIRIS S2000 product itself, creating a private cloud for the data that keeps the data within the customer's control only.<sup>6</sup> The second option is the data can be stored “remotely in Datto's secure cloud.”<sup>7</sup>

<sup>1</sup> According to Datto's website, its SIRIS product supports “business continuity” with server backups, virtualization, and cloud-based accessibility. See Datto Siris 2, found at <http://www.datto.com/siris>.

<sup>2</sup> Platte River Networks Invoice #7942 (May 31, 2013) (on file with the Committee on Homeland Security and Governmental Affairs).

<sup>3</sup> Datto, Inc., About Datto, <http://www.datto.com/about>.

<sup>4</sup> Datto SIRIS Brochure found at

[http://www.abletek.com/productcatalog/datto/siris/pdf/DattoSIRISProductBrochure\\_r2.pdf](http://www.abletek.com/productcatalog/datto/siris/pdf/DattoSIRISProductBrochure_r2.pdf).

<sup>5</sup> Instant Virtualization, Datto (last accessed on Sept. 23, 2015) <http://www.datto.com/technologies/instant-virtualization>.

<sup>6</sup> *Id.*

<sup>7</sup> *Id.*

Mr. Austin McChord  
October 5, 2015  
Page 2

According to information received by the Committee, Platte River Networks (PRN)<sup>8</sup> billed the Clinton Executive Service Corp. (CESC) on May 31, 2013, to acquire a Datto SIRIS S2000 device. CESC appears to be a Clinton family company. According to documents received by the Committee, CESC oversaw contracting for the hardware and software required for Secretary Clinton's private server and email.<sup>9</sup>

When Secretary Clinton's private server was moved from her private residence to the New Jersey-based data center, PRN set up the Datto SIRIS device at this new location.<sup>10</sup> When acquiring the Datto SIRIS product, it appears that CESC representatives worked with PRN employees to determine how the Datto device would back up data on Secretary Clinton's private server.<sup>11</sup> According to documents received by the Committee, CESC chose to only store the backup data on-site on the Datto SIRIS device, thus creating a private cloud managed by PRN.<sup>12</sup> CESC specifically requested that no data be stored on Datto's off-site cloud at any time.<sup>13</sup>

Although Secretary Clinton apparently wanted "Datto options *without* offsite backup," there was confusion among PRN employees when they noticed that data from Secretary Clinton's private server was potentially being sent to Datto's off-site backup location.<sup>14</sup> In

<sup>8</sup> Platte River Networks was hired by Secretary Clinton in 2013 to maintain the data stored on her private server.

<sup>9</sup> Email from Infograte to Platte River Networks (Apr. 17, 2013) (on file with the Committee on Homeland Security and Governmental Affairs).

<sup>10</sup> Platte River Networks Invoice #33427 (June 15, 2013) (on file with the Committee on Homeland Security and Governmental Affairs).

<sup>11</sup> See Email from Platte River Networks to Datto, Inc. (June 6, 2013) (on file with the Committee on Homeland Security and Governmental Affairs); Email from Platte River Networks to Platte River Networks (Jan. 26, 2015); Email from Platte River Networks to Platte River Networks (Jan. 26, 2015).

<sup>12</sup> Email from Platte River Networks to Datto, Inc. (June 6, 2013) (on file with the Committee on Homeland Security and Governmental Affairs). PRN billed for work installing the device in June 2013. For use of the private cloud capability, Datto charges a monthly fee. Each month beginning in July 2013, PRN billed CESC for "Datto Month of Private Cloud Service." This monthly service fee apparently allowed Secretary Clinton to continually have a backup on a private, virtual cloud on the SIRIS S2000 device. See Platte River Networks Invoice #33427 (June 15, 2013); Platte River Networks Invoice #33488 (June 17, 2013); Platte River Networks Invoice #IS.1307006 (July 1, 2013); Platte River Networks Invoice #IB.1308057 (Aug. 5, 2013); Platte River Networks Invoice #IB.1309050 (Sept. 4, 2013); Platte River Networks Invoice #IB.1310031 (Oct. 3, 2013); Platte River Networks Invoice #IB.1311027 (Nov. 5, 2013); Platte River Networks Invoice #IB.1312009 (Dec. 4, 2013); Platte River Networks Invoice #IB.1401012 (Jan. 6, 2014); Platte River Networks Invoice #IB.1402022 (Feb. 3, 2014); Platte River Networks Invoice #IB.1403010 (Mar. 3, 2014); Platte River Networks Invoice #IB.1404011 (Apr. 1, 2014); Platte River Networks Invoice #IB.1405011 (May 1, 2014); Platte River Networks Invoice #IB.1406011 (June 1, 2014); Platte River Networks Invoice #IB.1407012 (July 1, 2014); Platte River Networks Invoice #IB.1408012 (Aug. 4, 2014); Platte River Networks Invoice #IB.1409013 (Sept. 3, 2014); Platte River Networks Invoice #IB.1410015 (Oct. 1, 2014); Platte River Networks Invoice #IB.1411016 (Nov. 3, 2014); Platte River Networks Invoice #IB.1412015 (Dec. 2, 2013); Platte River Networks Invoice #IB.1501015 (Jan. 6, 2015); Platte River Networks Invoice #IB.1502014 (Feb. 2, 2015); Platte River Networks Invoice #IB.1503016 (Mar. 3, 2015); Platte River Networks Invoice #IB.1504014 (Apr. 1, 2015); Platte River Networks Invoice #IB.1505016 (May 1, 2015); Platte River Networks Invoice #IB.1506014 (June 1, 2015); Platte River Networks Invoice #IB.1507017 (July 1, 2015); Platte River Networks Invoice #IB.1508019 (Aug. 1, 2015) (all invoices mentioned on file with the Committee on Homeland Security and Governmental Affairs).

<sup>13</sup> Email from Platte River Networks to Datto, Inc. (June 6, 2013) (on file with the Committee on Homeland Security and Governmental Affairs).

<sup>14</sup> Email from Platte River Networks to Platte River Networks (Aug. 1, 2013) (on file with the Committee on Homeland Security and Governmental Affairs).

Mr. Austin McChord

October 5, 2015

Page 3

August 2015, employees at PRN discovered that Secretary Clinton's private server was syncing with "an offsite sync server . . . belonging to Datto."<sup>15</sup>

PRN employees reached out to Datto to determine if the server was actually sending data from the private server to Datto's off-site cloud for backup. One PRN employee wrote to Datto and stated, "[w]hen we made the purchase [of the SIRIS S2000], it was under the understanding that we didn't want to backup to Datto's [off-site] datacenter."<sup>16</sup> When a Datto employee determined that "for some reason this device [the SIRIS S2000] does appear to be syncing with the Datto Cloud,"<sup>17</sup> another PRN employee bluntly replied, "[t]his is a problem. This data should not be stored in the Datto Cloud . . ."<sup>18</sup> Whereas CESC specifically requested that no data from Secretary Clinton's private server be backed up off-site, according to this information, it appears that Datto was providing backups for the server "from the beginning" of the contract.<sup>19</sup> Thus, as of August 2015, Datto apparently possessed a backup of the server's contents since June 2013.

In response to this finding, PRN employees directed Datto to not delete the saved data and worked with Datto to find a way to move the saved information on Datto's servers back to Secretary Clinton's private server.<sup>20</sup> According to documents received by the Committee, it appears that Datto and PRN employees discussed an option to save the data on a USB drive, send the USB drive to PRN, and "then wipe [the data] from the [Datto] cloud."<sup>21</sup> Despite these communications, it is unclear whether or not this course of action was followed. Additionally, questions still remain as to whether Datto actually transferred the data from its off-site datacenter to the on-site server, what data was backed up, and whether Datto wiped the data after it was transferred.

It also appears that PRN employees were directed by CESC to reduce how much data would be stored in each backup. In August 2015, a PRN employee raised the prospect that the length of the backups was reduced at some point during PRN's time managing the server. In an email to a colleague with the subject line "CESC Datto," the PRN employee asked if it is possible to use Mimecast,<sup>22</sup> PRN's email archiving system, to find an old email from CESC directing PRN to reduce the length of Datto's backups. He wrote:

---

<sup>15</sup> Email from Platte River Networks to Platte River Networks (Aug. 6, 2015) (on file with the Committee on Homeland Security and Governmental Affairs).

<sup>16</sup> Email from Platte River Networks to Datto, Inc. (Aug. 6, 2015) (on file with the Committee on Homeland Security and Governmental Affairs).

<sup>17</sup> *Id.*

<sup>18</sup> *Id.*

<sup>19</sup> Email from Platte River Networks to Platte River Networks (Aug. 7, 2015) (on file with the Committee on Homeland Security and Governmental Affairs).

<sup>20</sup> Email from Platte River Networks to Datto, Inc. (Aug. 6, 2015) (on file with the Committee on Homeland Security and Governmental Affairs).

<sup>21</sup> Email from Platte River Networks to Platte River Networks (Aug. 7, 2015) (on file with the Committee on Homeland Security and Governmental Affairs).

<sup>22</sup> PRN used a Mimecast product that allowed PRN to archive employee emails in a cloud-based server and search that archive as needed. See Mimecast, Archiving, Risk & Compliance (last accessed on Sept. 23, 2015) <https://www.mimecast.com/solutions/email-archiving-compliance/>.

Mr. Austin McChord  
October 5, 2015  
Page 4

Any chance you found an old email with their directive to cut the backup back in Oct-Feb. I know they had you cut it once in Oct-Nov, then again to 30days [sic] in Feb-ish. If we had that email, we are golden. Would Mimecast have archived it by chance? Wondering how we can sneak an email in now after the fact asking them when they told us to cut the backups and have them confirm it for our records. Starting to think this whole thing really is covering up some shady shit.... I just think if we have it in writing that they told us to cut the backups, and that we can go public with our statement saying we have had backups since day one, then we were told to trim to 30days [sic], it would make us look a WHOLE LOT better.<sup>23</sup>

The State Department formally requested all of Secretary Clinton's records related to her time as Secretary of State on October 28, 2014.<sup>24</sup> It is unclear why Secretary Clinton's representatives apparently directed PRN to reduce the backup time period of her emails around the same time period or in the months following the State Department's request.

In order to better understand Datto's role relating to Secretary Clinton's private server, the backup and security capabilities of the private server, and any directives provided to Datto relating to the server, I ask that you please provide the following information and materials:

1. Please produce all documents and communications between or among employees or contractors of Datto and employees of Platte River Networks, Clinton Executive Services Corp. (CESC), or any other party referring or relating to Secretary Clinton's private server or any backup device.
2. Please produce all contracts between Datto and Platte River Networks, CESC, or any other party referring or relating to Secretary Clinton's private server or any backup device.
3. Please produce all invoices, bills, and receipts prepared by Datto or its representatives or agents regarding Secretary Clinton's private server or any backup device.
4. Please produce all helpdesk, service, or support tickets received by Datto from Platte River Networks, CESC, or any other party related to the Datto device used to backup Secretary Clinton's private server.
5. Is Datto authorized to store classified information? Were any Datto employees authorized to view classified information? Please explain. Did Datto's contract

---

<sup>23</sup> Email from Platte River Networks to Platte River Networks (Aug. 19, 2015) (emphasis added) (on file with the Committee on Homeland Security and Governmental Affairs); *see also* Email from Platte River Networks to Platte River Networks (Aug. 18, 2015) (PRN employee believes CESC direction to reduce the length of time backups were kept "was all phone comm[unication]s") (on file with the Committee on Homeland Security and Governmental Affairs).

<sup>24</sup> Letter from Patrick F. Kennedy, Under Secretary, U.S. Department of State, to Cheryl Mills (stamped Nov. 12, 2014) <http://www.archives.gov/press/press-releases/2015/pdf/attachment4-clinton-letter.pdf>.

regarding Secretary Clinton's private server include provisions related to the storing of classified information?

6. Has Datto been contacted by the Federal Bureau of Investigation (FBI) or any other law-enforcement entity regard Secretary Clinton's private server? Has Datto turned over any information, materials, or equipment to the FBI or any other law enforcement entity? Please explain.
7. Information obtained by the Committee suggests that PRN ordered a new Datto device in 2015 "to turn encryption on for the backups and then to power down the old device."<sup>25</sup> Please explain the measures taken to ensure the security of data stored on the SIRIS S2000 device, the private cloud, and the Datto Cloud.
  - a. Was the backup data stored on the private cloud encrypted when the device was first installed in 2013?
  - b. Was the backup data stored on the Datto Cloud encrypted?
8. Please explain the process for storing data in the Datto Cloud.
  - a. How long is data retained in the cloud?
  - b. What happens to the data once the required retention period is reached?
  - c. Is the data deleted automatically?
  - d. As mentioned above, CESC requested that the retention period for backups be reduced to 30 days. What information would be lost by reducing the backup retention period to 30 days? Please explain.
9. According to documents received by the Committee, Datto was providing off-site, cloud-based, back-up services for data contained on Secretary Clinton's private server.<sup>26</sup>
  - a. How much data was stored on Datto's cloud? Please explain.
  - b. Was this data eventually moved elsewhere? If so, where and how was this data moved? If the data was moved from Datto's servers, did Datto retain a copy of that data? If Datto retained a copy, please provide this material to the Committee.
  - c. Please explain what security measures are in place to protect the data stored on Datto's cloud?
  - d. During the time in which Secretary Clinton's private server was backed up on Datto's cloud, did Datto's cloud come under cyberattack? If so, please provide documentation that includes information about the time and date each attack occurred and whether any data was compromised.
  - e. According to documents received by the Committee, Datto was not supposed to be storing data from Secretary Clinton's private server as part of the contract.<sup>27</sup> Please explain how and why data was stored on Datto's cloud.

---

<sup>25</sup> Email from Platte River Networks to Platte River Networks (Aug. 18, 2015) (on file with the Committee on Homeland Security and Governmental Affairs).

<sup>26</sup> Email from Channel Sales Executive, Datto, Inc., to Platte River Networks (Aug. 6, 2015) (on file with the Committee on Homeland Security and Governmental Affairs).

Mr. Austin McChord  
October 5, 2015  
Page 6

- f. As mentioned above, Datto employees reviewed why backups to the Datto cloud were occurring.<sup>28</sup> Please provide any documentation or correspondence related to what these employees found.

Please provide this information and material as soon as possible, but no later than 5:00pm on October 19, 2015. Additionally, I ask that you please provide the Committee with a staff-level briefing to discuss Datto's role in backing up the server.

The Committee on Homeland Security and Governmental Affairs is authorized by Rule XXV of the Standing Rules of the Senate to investigate "the efficiency, economy, and effectiveness of all agencies and departments of Government."<sup>29</sup> Additionally, S. Res. 73 (114th Congress) authorizes the Committee to examine "the efficiency and economy of operations of all branches and functions of the Government with particular reference to (i) the effectiveness of present national security methods, staffing and processes..."<sup>30</sup> For purposes of this request, please refer to the definitions and instructions in the enclosure. To the maximum extent possible, please provide unclassified responses to my questions; should a complete response to any question require that you send me classified information, you may send me that information under separate cover, via the Office of Senate Security.

If you have any questions about this request, or concerns about the instructions or requirements in the enclosure, please contact Scott Wittmann or Mike Lueptow of the Committee staff at (202) 224-4751. Thank you for your prompt attention to this matter.

Sincerely,



Ron Johnson  
Chairman

cc: The Honorable Thomas R. Carper  
Ranking Member

Enclosure

---

<sup>27</sup> Email from Channel Sales Executive, Datto, Inc., to Platte River Networks (Aug. 6, 2015) (on file with the Committee on Homeland Security and Governmental Affairs).

<sup>28</sup> *Id.*

<sup>29</sup> S. Rule XXV(k); *see also* S. Res. 445, 108<sup>th</sup> Cong. (2004).

<sup>30</sup> S. Res. 73 § 12, 114<sup>th</sup> Cong. (2015).

**Instructions for Responding to a Committee Request**  
Committee on Homeland Security and Governmental Affairs  
United States Senate  
114th Congress

**A. Responding to a Request for Documents**

1. In complying with the Committee's request, produce all responsive documents that are in your possession, custody, or control, whether held by you or your past or present agents, employees, and representatives acting on your behalf. You should also produce documents that you have a legal right to obtain, that you have a right to copy or to which you have access, as well as documents that you have placed in the temporary possession, custody, or control of any third party. Requested records, documents, data, or information should not be destroyed, modified, removed, transferred, or otherwise made inaccessible to the Committee.
2. In the event that any entity, organization, or person denoted in the request has been or is also known by any other name or alias than herein denoted, the request should be read also to include the alternative identification.
3. The Committee's preference is to receive documents in electronic form (i.e. CD, memory stick, or thumb drive) in lieu of paper productions.
4. Documents produced in electronic form should also be organized, identified, and indexed electronically.
5. Electronic document productions should be prepared according to the following standards:
  - a. The production should consist of single page Tagged Image Files (".tif"), files accompanied by a Concordance-format load file, an Opticon reference file, and a file defining the fields and character lengths of the load file.
  - b. Document numbers in the load file should match document Bates numbers and .tif file names.
  - c. If the production is completed through a series of multiple partial productions, field names and file order in all load files should match.
  - d. All electronic documents produced should include the following fields of metadata specific to each document:

BEGDOC, ENDDOC, TEXT, BEGATTACH, ENDATTACH, PAGECOUNT, CUSTODIAN, RECORDTYPE, DATE, TIME, SENTDATE, SENTTIME, BEGINDATE, BEGINTIME, ENDDATE, ENDTIME, AUTHOR, FROM, CC, TO, BCC, SUBJECT, TITLE, FILENAME, FILEEXT, FILESIZE, DATECREATED, TIMECREATED, DATELASTMOD, TIMELASTMOD, INTMSGID, INTMSGHEADER, NATIVELINK, INTFILPATH, EXCEPTION, BEGATTACH.

## Instructions for Responding to a Committee Request

- e. Alternatively, if the production cannot be made in .tif format, all documents derived from word processing programs, email applications, instant message logs, spreadsheets, and wherever else practicable should be produced in text searchable Portable Document Format (".pdf") format. Spreadsheets should also be provided in their native form. Audio and video files should be produced in their native format, although picture files associated with email or word processing programs should be produced in .pdf format along with the document it is contained in or to which it is attached.
  - f. If any of the requested information is only reasonably available in machine-readable form (such as on a computer server, hard drive, or computer backup tape), consult with the Committee staff to determine the appropriate format in which to produce the information.
6. Documents produced to the Committee should include an index describing the contents of the production. To the extent more than one CD, hard drive, memory stick, thumb drive, box or folder is produced, each CD, hard drive, memory stick, thumb drive, box or folder should contain an index describing its contents.
  7. Documents produced in response to the request should be produced together with copies of file labels, dividers or identifying markers with which they were associated when the request was served.
  8. When producing documents, identify the paragraph in the Committee's schedule to which the documents respond.
  9. Do not refuse to produce documents on the basis that any other person or entity also possesses non-identical or identical copies of the same documents.
  10. This request is continuing in nature and applies to any newly discovered information. Any record, document, compilation of data or information not produced because it has not been located or discovered by the return date, should be produced immediately upon subsequent location or discovery.
  11. All documents should be Bates-stamped sequentially and produced sequentially. Each page should bear a unique Bates number.
  12. Two sets of documents should be delivered, one set to the Majority Staff and one set to the Minority Staff. When documents are produced to the Committee, production sets should be delivered to the Majority Staff in Room 340 of the Dirksen Senate Office Building and the Minority Staff in Room 346 of the Dirksen Senate Office Building.
  13. If compliance with the request cannot be made in full by the date specified in the request, compliance should be made to the extent possible by that date. Notify Committee staff as soon as possible if full compliance cannot be made by the date specified in the request, and provide an explanation for why full compliance is not possible by that date.

### **Instructions for Responding to a Committee Request**

14. In the event that a document is withheld on the basis of privilege, provide a privilege log containing the following information concerning any such document: (a) the privilege asserted; (b) the type of document; (c) the general subject matter; (d) the date, author and addressee; and (e) the relationship of the author and addressee to each other.
15. If any document responsive to this request was, but no longer is, in your possession, custody, or control, identify the document (stating its date, author, subject and recipients) and explain the circumstances under which the document ceased to be in your possession, custody, or control.
16. If a date or other descriptive detail set forth in this request referring to a document is inaccurate, but the actual date or other descriptive detail is known to you or is otherwise apparent from the context of the request, produce all documents which would be responsive as if the date or other descriptive detail were correct.
17. In the event a complete response requires the production of classified information, provide as much information in unclassified form as possible in your response and send all classified information under separate cover via the Office of Senate Security.
18. Unless otherwise specified, the period covered by this request is from January 1, 2009 to the present.
19. Upon completion of the document production, you should submit a written certification, signed by you or your counsel, stating that: (1) a diligent search has been completed of all documents in your possession, custody, or control which reasonably could contain responsive documents; and (2) all documents located during the search that are responsive have been produced to the Committee.

### **B. Responding to Interrogatories or a Request for Information**

1. In complying with the Committee's request, answer truthfully and completely. Persons that knowingly provide false testimony could be subject to criminal prosecution for perjury (when under oath) or for making false statements. Persons that knowingly withhold subpoenaed information could be subject to proceedings for contempt of Congress. If you are unable to answer an interrogatory or information request fully, provide as much information as possible and explain why your answer is incomplete.
2. In the event that any entity, organization, or person denoted in the request has been or is also known by any other name or alias than herein denoted, the request should be read also to include the alternative identification.
3. Your response to the Committee's interrogatories or information requests should be made in writing and should be signed by you, your counsel, or a duly authorized designee.

**Instructions for Responding to a Committee Request**

4. When responding to interrogatories or information requests, respond to each paragraph in the Committee's schedule separately. Clearly identify the paragraph in the Committee's schedule to which the information responds.
5. Where knowledge, information, or facts are requested, the request encompasses knowledge, information or facts in your possession, custody, or control, or in the possession, custody, or control of your staff, agents, employees, representatives, and any other person who has possession, custody, or control of your proprietary knowledge, information, or facts.
6. Do not refuse to provide knowledge, information, or facts on the basis that any other person or entity also possesses the same knowledge, information, or facts.
7. The request is continuing in nature and applies to any newly discovered knowledge, information, or facts. Any knowledge, information, or facts not provided because it was not known by the return date, should be provided immediately upon subsequent discovery.
8. Two sets of responses should be delivered, one set to the Majority Staff and one set to the Minority Staff. When responses are provided to the Committee, copies should be delivered to the Majority Staff in Room 340 of the Dirksen Senate Office Building and the Minority Staff in Room 346 of the Dirksen Senate Office Building.
9. If compliance with the request cannot be made in full by the date specified in the request, compliance should be made to the extent possible by that date. Notify Committee staff as soon as possible if full compliance cannot be made by the date specified in the request, and provide an explanation for why full compliance is not possible by that date.
10. In the event that knowledge, information, or facts are withheld on the basis of privilege, provide a privilege log containing the following information: (a) the privilege asserted; (b) the general subject matter of the knowledge, information, or facts withheld; (c) the source of the knowledge, information, or facts withheld; (d) the paragraph in the Committee's request to which the knowledge, information, or facts are responsive; and (e) each individual to whom the knowledge, information, or facts have been disclosed.
11. If a date or other descriptive detail set forth in this request is inaccurate, but the actual date or other descriptive detail is known to you or is otherwise apparent from the context of the request, provide the information that would be responsive as if the date or other descriptive detail was correct.
12. In the event a complete response requires the transmission of classified information, provide as much information in unclassified form as possible in your response and send all classified information under separate cover via the Office of Senate Security.
13. Unless otherwise specified, the period covered by this request is from January 1, 2009 to the present.

## Instructions for Responding to a Committee Request

### C. Definitions

1. The term “document” in the request or the instructions means any written, recorded, or graphic matter of any nature whatsoever, regardless of how recorded, and whether original or copy, including, but not limited to, the following: memoranda, reports, expense reports, books, manuals, instructions, financial reports, working papers, records, notes, letters, notices, confirmations, telegrams, receipts, appraisals, pamphlets, magazines, newspapers, prospectuses, inter-office and intra-office communications, electronic mail (e-mail), contracts, cables, notations of any type of conversation, telephone call, meeting or other communication, bulletins, printed matter, computer printouts, teletypes, invoices, transcripts, diaries, analyses, returns, summaries, minutes, bills, accounts, estimates, projections, comparisons, messages, correspondence, press releases, circulars, financial statements, reviews, opinions, offers, studies and investigations, questionnaires and surveys, and work sheets (and all drafts, preliminary versions, alterations, modifications, revisions, changes, and amendments of any of the foregoing, as well as any attachments or appendices thereto), and graphic or oral records or representations of any kind (including without limitation, photographs, charts, graphs, microfiche, microfilm, videotape, recordings and motion pictures), and electronic, mechanical, and electric records or representations of any kind (including, without limitation, tapes, cassettes, disks, and recordings) and other written, printed, typed, or other graphic or recorded matter of any kind or nature, however produced or reproduced, and whether preserved in writing, film, tape, disk, videotape or otherwise. A document bearing any notation not a part of the original text is to be considered a separate document. A draft or non-identical copy is a separate document within the meaning of this term.
2. The term “communication” in the request or the instructions means each manner or means of disclosure or exchange of information, regardless of means utilized, whether oral, electronic, by document or otherwise, and whether face to face, in meetings, by telephone, mail, telex, facsimile, email (desktop or mobile device), computer, text message, instant message, MMS or SMS message, regular mail, telexes, discussions, releases, delivery, or otherwise.
3. The terms “and” and “or” in the request or the instructions should be construed broadly and either conjunctively or disjunctively to bring within the scope of this subpoena any information which might otherwise be construed to be outside its scope. The singular includes plural number, and vice versa. The masculine includes the feminine and neuter genders.
4. The terms “person” or “persons” in the request or the instructions mean natural persons, firms, partnerships, associations, corporations, subsidiaries, divisions, departments, joint ventures, proprietorships, syndicates, or other legal, businesses or government entities, and all subsidiaries, affiliates, divisions, departments, branches, or other units thereof.
5. The term “identify” in the request or the instructions, when used in a question about individuals, means to provide the following information: (a) the individual’s complete name and title; and (b) the individual’s business address and phone number.

**Instructions for Responding to a Committee Request**

6. The terms “referring” or “relating” in the request or the instructions, when used separately or collectively, with respect to any given subject, mean anything that constitutes, contains, embodies, reflects, identifies, states, refers to, deals with or is pertinent to that subject in any manner whatsoever.
7. The term “employee” in the request or the instructions means agent, borrowed employee, casual employee, consultant, contractor, de fact employee, independent contractor, joint adventurer, loaned employee, part-time employee, permanent employee, provisional employee or subcontractor.
8. The terms “you” and “your” in the request or the instructions refer to yourself; your firm, corporation, partnership, association, department, or other legal or government entity, including all subsidiaries, divisions, branches, or other units thereof; and all members, officers, employees, agents, contractors, and all other individuals acting or purporting to act on your behalf, including all present and former members, officers, employees, agents, contractors, and all other individuals exercising or purporting to exercise discretion, make policy, and/or decisions.

# # #

**EXHIBIT B**



BOSTON CONNECTICUT NEW JERSEY NEW YORK WASHINGTON, DC

STANLEY A. TWARDY, JR.  
Attorney at Law

One Canterbury Green  
Stamford, CT 06901-2047  
T: (203) 977-7368 F: (866) 458-1037  
satwardy@daypitney.com

October 19, 2015

**VIA UPS**

The Honorable Ron Johnson  
Chairman  
Committee on Homeland Security & Governmental Affairs  
United States Senate  
Washington, D.C., 20510

The Honorable Thomas R. Carper  
Ranking Member  
Committee on Homeland Security & Governmental Affairs  
United States Senate  
Washington, D.C., 20510

Dear Chairman Johnson and Ranking Member Carper:

We represent Datto, Inc., (“Datto”) and write further to our October 7, 2015 letter in response to Chairman Johnson’s letter to Datto Chief Executive Officer Mr. Austin McChord dated October 5, 2015.

In your October 5<sup>th</sup> letter, you requested that Datto voluntarily provide certain information to assist the Committee to “better understand Datto’s role relating to Secretary Clinton’s private server, the backup and security capabilities of the private server, and any directives provided to Datto relating to the server.”<sup>1</sup> This letter responds to those requests and reiterates Datto’s intention to continue responding to and complying with the requests in your letter, to the extent permitted by Datto’s data privacy policies and its contractual confidentiality requirements.

<sup>1</sup> Letter from The Honorable Ron Johnson to Mr. Austin McChord, dated October 5, 2015, at p. 4. It is our understanding that your request contemplates a voluntary response, and that no subpoena has issued pursuant to the *Rules of Procedure of the Committee on Homeland Security and Governmental Affairs*, March 2015.

The Honorable Ron Johnson  
The Honorable Thomas R. Carper  
October 19, 2015  
Page 2

The relevant terms of those requirements as stated in a typical Reseller Agreement include:

“Confidential Information” means any information, whether oral, written, electronic, or in any other format, and whether technical or business in nature, regarding this Agreement, Datto’s products or business, including the Product, information regarding a party’s products, services, Marks, software, intellectual property, equipment, pricing, marketing and business plans, other information not generally known to the public and any other information received under circumstances reasonably interpreted as imposing an obligation of confidentiality; provided that, “Confidential Information” shall not include any of such information which: (i) was publicly available at the time of disclosure by the disclosing party; (ii) became publicly available after disclosure through no fault of the receiving party; (iii) was known to the receiving party prior to disclosure by the disclosing party; or (iv) was rightfully acquired by the receiving party after disclosure by the disclosing party from a third party who was lawfully in possession of the information and was under no legal duty to the disclosing party to maintain the confidentiality of the information.

*Required Disclosures.* Either party may disclose Confidential Information to the extent disclosure is based on the good faith written opinion of such party’s legal counsel that disclosure is required by law or by order of a court or governmental agency; provided that, the party that is the recipient of such Confidential Information shall use all commercially reasonable efforts to maintain the confidentiality of the Confidential Information by means of a protective order or other similar protection and shall give the owner of such Confidential Information prompt notice in order that it have every opportunity to intercede in such process to contest such disclosure and shall use all commercially reasonable efforts to cooperate with the owner of such Confidential Information to protect the confidentiality of such Confidential Information. The owner of such Confidential Information reserves the right to obtain a protective order or otherwise protect the confidentiality of such Confidential Information.

On October 6, 2015, in accordance with its obligations under the Reseller Agreement, Datto notified Platte River Networks (“Platte River”) of your October 5 inquiry, and asked whether they would object to disclosure of the information and materials requested. Platte River advised us that they had “no objection.” However, on October 14, 2015, counsel to Platte River withdrew their previous non-objection, and objected to any further disclosure of Confidential Information (as defined in the Reseller Agreement) to the Committee. Accordingly, Datto cannot disclose any such Confidential Information unless required by law or by order of a court or governmental agency.

The Honorable Ron Johnson  
The Honorable Thomas R. Carper  
October 19, 2015  
Page 3

Our review of documents and other materials related to your requests continue, and should that effort reveal additional information responsive to your requests that is not confidential, we will supplement this response.

## I. BACKGROUND

Datto is a back-end service provider to thousands of managed IT service providers – often referred to as Managed Service Providers (“MSPs”) or “Resellers” such as Platte River. MSPs are often sophisticated, professional companies that provide a defined set of IT operations and services to their clients or “End-Users.” Datto works almost exclusively with these MSPs to provide comprehensive and secure “hybrid cloud” backup, data recovery, and business continuity solutions that the MSPs in turn resell and administer to End-Users. To accomplish this, Datto provides hardware, software and technical services to MSPs, as more fully described below. Datto also provides MSP customers with training on how to use Datto services.

Datto’s services to MSPs are generally governed by Reseller Agreements between the MSP and Datto. These contracts contain mutual and binding confidentiality clauses. As previously discussed, such a clause applies in Datto’s contract with Platte River. Rarely does Datto deal directly with an End-User, and in the matter referred to in your inquiry, Datto’s contractual relationship was with Platte River only. Datto was not aware of the identity of the End-User until reading allegations in the media.

Datto’s hybrid cloud solution involves two parts: (i) a local hardware backup device, such as the Datto SIRIS device (a “Local Device”); and (ii) a replicated offsite backup.<sup>2</sup> First, the Datto solution uses software to take a full backup image of the End-User’s IT environment that is being backed up (servers, data, etc.) and copies it onto a Local Device, which is a hardware device that is often located in the same physical location as the IT environment it is backing up (i.e. the “server room”). From there, the Local Device works as a “failover” system in the event of a business interruption that impacts the End-User’s IT environment. Second, a duplicate copy of all of the information stored on the Local Device is also placed on a replicated storage device (a “Storage Node”) that is located at a different location (i.e. “offsite”) than the Local Device.<sup>3</sup> Offsite replication ensures that if the event that caused the End-User’s system to fail also impacts the Local Device (e.g. a fire or flood) the MSP can use the cloud – “Datto Cloud” or a “Private Cloud” – as an alternative failover system from the Local Device.

In most use cases, the MSP chooses for offsite replication to occur at a Datto-controlled data center facility. Datto refers to this approach as a “Datto Cloud” solution. In other use cases,

---

<sup>2</sup> In this letter “local” refers to the physical location of the MSP’s systems.

<sup>3</sup> This duplication is accomplished by the creation of multiple restore points that can be individually reconstructed to restore the dataset as it previously existed at a particular time.

The Honorable Ron Johnson  
The Honorable Thomas R. Carper  
October 19, 2015  
Page 4

MSPs may choose to replicate backed-up data offsite to a Storage Node owned and operated by the MSP at a site of its choosing. Datto refers to this approach as a “Private Cloud.”

As an alternative to a hybrid cloud approach, an MSP may opt out of offsite replication altogether and request a “Local Only” setup. In a Local Only configuration, backed-up data will not replicate beyond the Local Device. Because Datto’s technology solution is meant to be deployed as a hybrid cloud solution, to set up a Local Only solution, generally the MSP must work directly with Datto technical support to implement this. By default, absent a functioning private offsite Storage Node or the requisite communications with Datto technical support, all Local Devices replicate to the Datto Cloud.

As noted, as a back-end service provider, Datto very rarely—if ever—has any direct interaction with the End-Users served by the MSPs. The nature of Datto’s relationship with MSPs precludes Datto from knowing either the identity of End-Users and the content of the data stored on the Local Device or replicated offsite. Datto has no role in monitoring the content or source of data stored by MSP clients such as Platte River. As such, Datto would not be aware of who was Platte River’s End-User and Datto did not and does not have any knowledge concerning the content of any data that may or may not have been backed up to the Datto Cloud, or stored on the Datto SIRIS device owned and operated by Platte River.<sup>4</sup>

## II. DATTO INVOLVEMENT IN MATTERS RELATED TO THE COMMITTEE’S INQUIRY

Datto first became aware that Platte River had been contacted by U.S. Government officials inquiring into Platte River’s involvement with former Secretary Clinton’s e-mail server through media reports on or about Sunday, August 9, 2015. Soon thereafter, Datto disconnected the replicated offsite Storage Node, and independently took prudential steps to preserve information within Datto’s control which Datto believed could be subject to law enforcement or other governmental inquiry.

On September 10, 2015, Datto received a *Request for Preservation of Records* from the Federal Bureau of Investigation (FBI) requesting that Datto preserve records related to a Datto Local Device identified by the FBI. Datto informed the FBI on September 16, 2015 that Datto had disconnected and preserved an offsite Storage Node associated with the Local Device. On October 6, 2015, with the consent of Platte River and its End-User, Datto provided the Storage Node to the FBI. The FBI has custody of the Storage Node.

---

<sup>4</sup> Datto’s standard contracts permit communication with an End-User, but this rarely is done, and was not in this case. In rare cases, Datto will be asked to directly assist an End-User.

The Honorable Ron Johnson  
The Honorable Thomas R. Carper  
October 19, 2015  
Page 5

III. RESPONSES TO INFORMATION REQUESTS

Please note that with respect to questions 1-4, 7, 8 and 9, these requests call for the production of documents and materials that are Confidential Information as defined by the Datto Reseller Agreement and Datto's data privacy policies. Consequently, Datto is not authorized to disclose such information absent consent from its client, Platte River, or unless required by law or by order of court or governmental agency.

With respect to questions to which the immediately preceding paragraph does not apply, Datto responds as follows:

5. *Is Datto authorized to store classified information? Were any Datto employees authorized to view classified information? Please explain. Did Datto's contract regarding Secretary Clinton's private server include provisions related to the storing of classified information?*

**RESPONSE:** Datto is not authorized to store classified information, and does not offer storage of classified information as part of its business.<sup>5</sup> No Datto employees are authorized to access classified information in the context of their employment at Datto. Datto has never entered into any contracts containing provisions related to the storage of classified information.

6. *Has Datto been contacted by the Federal Bureau of Investigation (FBI) or any other law-enforcement entity regard (sic) Secretary Clinton's private server? Has Datto turned over any information, materials, or equipment to the FBI or any other law enforcement entity? Please explain.*

**RESPONSE:** On September 10, 2015, Datto received a *Request for Preservation of Records* from the FBI, requesting that Datto preserve records related to a Datto Local Device identified by the FBI. Datto informed the FBI on September 16, 2015 that Datto had disconnected and preserved an offsite Storage Node associated with the Local Device. On October 6, 2015, with the consent of Platte River and its End-User, Datto provided the Storage Node to the FBI. The FBI has custody of the Storage Node.

8. *Please explain the process for storing data in the Datto Cloud.*  
*a. How long is data retained in the cloud?*  
*b. What happens to the data once the required retention period is reached?*

---

<sup>5</sup> For purposes of this response "classified information" means information classified pursuant to Executive Order 13526. Datto does not hold a Facilities Clearance (FCL) as administered by the Defense Security Service, or any other U.S. Government agency or department.

The Honorable Ron Johnson  
The Honorable Thomas R. Carper  
October 19, 2015  
Page 6

- c. *Is the data deleted automatically?*
- d. *As mentioned above, CESC requested that the retention period for backups be reduced to 30 days. What information would be lost by reducing the backup retention period to 30 days? Please explain.*

**RESPONSE:** To the extent Chairman Johnson's request calls for a general outline of the process for storing data in the Datto Cloud, or Datto's security capabilities and functions, we note that Datto's security efforts include hardware, software, and encryption mechanisms as well as physical, technical and administrative controls. The details of these capabilities are confidential, and public disclosure of those details could reveal vulnerabilities and capabilities of Datto's systems, infrastructures, projects, plans, or protection services relating to its business and the data entrusted to Datto by its MSP customers. As such, public disclosure of these capabilities could cause Datto's systems to become less secure.

The Datto Cloud has over 140 petabytes of cloud storage capacity. Usage of that storage capacity fluctuates depending on the retention settings established by the MSP. That said, Datto's solution takes an exact and comprehensive backup image of the entire host machine that it backs up. The Datto solution will keep an image of everything that was on the host machine when the last backup was taken. Users generally take that image every day, usually more than once per day. The data is stored in a snapshot capable file system that tracks the state of the backups back in time. At any one point, the solution will have the most recent copy of the machine it backs up as well as a number of exact copies of prior versions depending on the retention settings that the MSP has chosen. If the retention settings are 30 days, that means that the picture the Datto Solution takes on day 1 will roll off the backup chain on day 31.

The following is an example of how a specific retention setting would apply to a theoretical unit of data. This example assumes a 30 day retention setting, and that user settings provide for only one full backup per day.

Day 1 – The backup includes a word document (“Document A”) that is sitting on the host machine.

Day 15 – Before the day's backup was taken, the user makes changes to Document A. Rather than saving the changes to a new word document, the user just writes over Document A.

Day 30 – The user realizes that she liked the way Document A was drafted before she wrote over it. The Datto solution took an image of Document A on each of days 1 through 14 (before it was written over). The user can retrieve that Document A from the backup images made on days 1 through 14.

 DAY PITNEY LLP

The Honorable Ron Johnson  
The Honorable Thomas R. Carper  
October 19, 2015  
Page 7

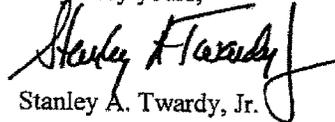
Day 60 – Assume that the user did not realize until day 60 that she liked the way Document A was drafted before she changed it. Document A is no longer recoverable because the last backup of that document would have dropped off the backup chain on day 44.

That said, an image based backup is a sparse file. It is a block by block copy of the host machine that it backs up. When data is removed from the file system, in most cases the file system does not automatically “zero out” the de-referenced blocks on a hard drive. Rather, a metadata store marks those blocks as free for future use. So, there remains a potential that de-referenced blocks of data may still reside on a hard drive.

#### IV. CONCLUSION

Thank you for the opportunity to assist the Committee in its work. Please do not hesitate to contact me if you have any questions.

Very truly yours,



Stanley A. Twardy, Jr.

cc: Michael Joseph Lueptow  
Investigative Counsel  
Committee on Homeland Security & Governmental Affairs  
United States Senate  
Washington, D.C., 20510  
*Via E-mail*

Scott D. Wittmann  
Investigative Counsel  
Committee on Homeland Security & Governmental Affairs  
United States Senate  
Washington, D.C., 20510  
*Via E-mail*

James Secreto  
Chief Counsel for Oversight and Investigations (Minority)  
Committee on Homeland Security & Governmental Affairs  
United States Senate  
Washington, D.C., 20510  
*Via E-mail*