(U) MEMORANDUM OF AGREEMENT

BETWEEN

AT&T

AND

THE DEPARTMENT OF HOMELAND SECURITY (DHS)
OFFICE OF CYBERSECURITY AND COMMUNICATIONS (CS&C)

FOR THE
JOINT CYBERSECURITY SERVICES PILOT (JCSP)

I. (U) PURPOSE AND SCOPE

A. (U//FOUO) This Memorandum of Agreement ("Agreement") between DHS and AT&T governs the U.S. Government's provision of and the AT&T's receipt and use of GFI and related activities in connection with the JCSP.

II. (U) RESPONSIBILITIES OF THE PARTIES

A. (U//FOUO) DHS, through the Office of Cybersecurity and Communications (CS&C) shall—

1. (U//FOUO) Provide classified and unclassified GFI to AT&T for use in an approved secure environment within its infrastructure for the purpose of offering specified managed security services to eligible critical infrastructure entities and U.S. Government agencies;
2. (U//FOUO) Provide AT&T with technical expertise regarding the use and protection of GFI, including recommending suitable managed security service offerings, consistent with the security guidelines provided under paragraph II.A.3 and Appendix A;
3. (U//FOUO) Provide to AT&T written security guidelines, developed in cooperation with the DOD, for the handling of GFI and implementation of specified managed security services in accordance with Appendix A;
4. (U//FOUO) Provide AT&T with updated lists of eligible critical infrastructure entities and U.S. Government agencies to whom managed security services under the JCSP may be offered;
5. (U//FOUO) Assist AT&T in decommissioning any classified equipment identified in accordance with paragraph II.B.6;
6. (U//FOUO) Accept, protect and hold in confidence all cybersecurity incident information that may be provided by AT&T pursuant to the CSP's agreements with its customers that are either critical infrastructure entities and U.S. Government agencies ;

7. (U//FOUO) Protect and hold in confidence any trade secrets or sensitive AT&T information provided under paragraph II.B.7 in accordance with this Agreement and its obligations under the law; and
8. (U//FOUO) Clearly identify through restrictive markings, notices, transmittal documents, or other appropriate means all GFI provided to AT&T so that such information can be protected as provided in this Agreement and to the full extent required by law.

B. (U//FOUO) If required by the terms of its contracts or other agreements with participating critical infrastructure entities and the U.S. Government entities, The CSP> agrees to—.

1. (U//FOUO) Accept unclassified and classified GFI from DHS to use in an approved secure environment within its infrastructure for the purpose of offering specified managed security services to such entities;
2. (U//FOUO) Handle and safeguard all GFI and derivative information associated with its work under this Agreement in accordance with the security guidelines that have been provided under paragraph II.A.3 and Appendix A;
3. (U//FOUO) Use GFI provided by DHS under this Agreement only for the purposes described in this Agreement;
4. (U//FOUO) Limit access to any classified GFI to AT&T support personnel with appropriate security clearances and need to know in accordance with the security guidelines that have been provided under paragraph II.A.3 and Appendix A;
5. (U//FOUO) Provide to DHS an inventory of company-owned classified equipment no longer needed for JCSP activity and follow all associated Government decommissioning instructions provided in accordance with paragraph A.6;
6. (U//FOUO) Identify through restrictive markings, notices, transmittal documents, or other appropriate means any personally identifiable information (PII), trade secrets or sensitive AT&T commercial, financial or technical information provided to DHS so that such information can be protected to the full extent authorized by law;
7. (U//FOUO) Permit, within normal business hours and upon at least 24 hours notice, U.S. Government security personnel to physically access AT&T network infrastructure as necessary for the protection of classified GFI in order to verify proper installation, logical configuration, and operation for security purposes;
8. (U//FOUO) Implement specified managed security service offerings for eligible critical infrastructure entities and U.S. Government agencies in accordance with guidelines provided under paragraph II.A.2 and Appendix A;

III. GENERAL PROVISIONS

A. (U//FOUO) This agreement does not promise present or future obligation of funds by the parties.

B. (U//FOUO)The existence of the Agreement and the activities to be conducted under it are intended to further efforts to use GFI to protect critical infrastructure entities and U.S. Government agencies and are not an endorsement of or approval by the Government of AT&T, or any of its products or services.

C. (U//FOUO) The information provided by the parties under this Agreement is provided without any guarantee, warranty, or assurance of its accuracy or effectiveness, whether express or implied, and the parties assume no liability for use of or reliance on information disclosed under this Agreement.

D. (U//FOUO) DHS authorizes, on behalf of the U.S. Government, use of the GFI provided under this Agreement by AT&T for the purposes described herein. If AT&T desires to obtain additional rights in such information beyond those needed for activities under Agreement, the parties will enter into good faith negotiations for any required license in accordance with federal law.

E. (U//FOUO) The parties will conduct their respective activities under this Agreement in accordance with applicable laws, including restrictions on the interception, monitoring, access, use, or sharing of electronic communications.

IV. POINTS OF CONTACT

A. (U//FOUO) DHS of Homeland Security point of contact is:

<NAME>
<TITLE>
Department of Homeland Security,
Office of Cybersecurity & Communications
<Contact information>

B. (U//FOUO) The AT&T point of contact is:

(b) (6)
Executive Director
AT&T
(b) (6)

V. (U) TERMINATION REVIEW

A. (U//FOUO) The parties reserve the right to unilaterally limit, discontinue, or terminate the activities under this Agreement upon written notice by either party.

B. Prior to termination, AT&T shall return to DHS or, at DHS's option, destroy all GFI provided to it by DHS and all classified information in AT&T's possession as a result of this Agreement, except for the Memorandum of Agreement, appendices thereto, and any associated written approvals thereunder.

C. Termination is the sole remedy under this Agreement for violation of its term and conditions; however, the rights and remedies of the parties that arise from any other source are not limited or affected by this Agreement. Neither party waives any right it may have as a matter of law or contract.

D. Termination of this Agreement does not relieve the parties of the obligation to protect against unauthorized disclosure any information received under this Agreement.

[redacted]

[redacted]
Executive Director

Name
Title

(U) MEMORANDUM OF AGREEMENT

BETWEEN

CenturyLink

AND

THE DEPARTMENT OF HOMELAND SECURITY (DHS)
OFFICE OF CYBERSECURITY AND COMMUNICATIONS (CS&C)

FOR THE
JOINT CYBERSECURITY SERVICES PILOT (JCSP)

I. (U) PURPOSE AND SCOPE

A. (U//FOUO) This Memorandum of Agreement ("Agreement") between the Department of Homeland Security (DHS) and Qwest Government Services Inc., dba CenturyLink – Government ("CenturyLink") governs the U.S. Government's provision of and the CenturyLink's receipt and use of U.S. Government furnished information (GFI) and related activities in connection with the Joint Cybersecurity Services Pilot (JCSP) to protect eligible critical infrastructure entities and U.S. Government agencies. The JCSP activities under this MOA are a continuation of those efforts previously initiated under an agreement between CenturyLink and the Department of Defense (DOD).

II. (U) RESPONSIBILITIES OF THE PARTIES

A. (U//FOUO) DHS, through the Office of Cybersecurity and Communications (CS&C) shall—

1. (U//FOUO) Provide classified and unclassified GFI to CenturyLink for use in an approved secure environment within its infrastructure for the purpose of offering specified managed security services to eligible critical infrastructure entities and U.S. Government agencies;
2. (U//FOUO) Provide CenturyLink with technical expertise regarding the use and protection of GFI, including suitable managed security service offerings, consistent with the security guidelines provided under paragraph II.A.3 and Appendix A;
3. (U//FOUO) Provide to CenturyLink written security guidelines, developed in cooperation with the DOD, for the handling of GFI and implementation of specified managed security services in accordance with Appendix A;
4. (U//FOUO) Provide CenturyLink with updated lists of eligible critical infrastructure entities and U.S. Government agencies to whom managed security services under the JCSP may be offered;

5. (U//FOUO) Assist CenturyLink in decommissioning any classified equipment identified in accordance with paragraph II.B.6;
6. (U//FOUO) Accept, protect and hold in confidence all cybersecurity incident information that may be provided by CenturyLink pursuant to the CenturyLink's agreements with its customers that are either eligible critical infrastructure entities and U.S. Government agencies in accordance with section III;
7. (U//FOUO) Protect and hold in confidence any trade secrets or sensitive CenturyLink information provided under paragraph II.B.7 in accordance with this Agreement and its obligations under the law; and
8. (U//FOUO) Clearly identify through restrictive markings, notices, transmittal documents, or other appropriate means all GFI provided to CenturyLink so that such information can be protected as provided in this Agreement and to the full extent required by law.

B. (U//FOUO) The CenturyLink shall—

1. (U//FOUO) Accept unclassified and classified GFI from DHS to use in an approved secure environment within its infrastructure for the purpose of offering specified managed security services to eligible critical infrastructure entities and U.S. Government agencies;
2. (U//FOUO) Handle and safeguard all GFI and derivative information associated with its work under this Agreement in accordance with the security guidelines that have been provided under paragraph II.A.3 and Appendix A;
3. (U//FOUO) Use GFI provided by DHS under this Agreement only for the purposes described in this Agreement;
4. (U//FOUO) Limit access to any classified GFI to CenturyLink support personnel with appropriate security clearances and need to know in accordance with the security guidelines that have been provided under paragraph II.A.3 and Appendix A;
5. (U//FOUO) Provide to DHS an inventory of company-owned classified equipment no longer needed for JCSP activity and follow all associated Government decommissioning instructions provided in accordance with paragraph A.6;
6. (U//FOUO) Identify through restrictive markings, notices, transmittal documents, or other appropriate means any personally identifiable information (PII), trade secrets or sensitive CenturyLink commercial, financial or technical information provided to DHS so that such information can be protected to the full extent authorized by law;
7. (U//FOUO) Permit, within normal business hours and upon at least 24 hours notice, U.S. Government security personnel to physically access CenturyLink network infrastructure as necessary for the protection of classified GFI in order to verify proper installation, logical configuration, and operation for security purposes;

8. (U//FOUO) Implement specified managed security service offerings for eligible critical infrastructure entities and U.S. Government agencies in accordance with guidelines provided under paragraph II.A.2 and Appendix A;
9. (U//FOUO) Ensure that contracts or other agreements with eligible critical infrastructure entities and U.S. Government agencies receiving managed cybersecurity services under the JCSP from CenturyLink are consistent with the terms of this Agreement.

III. CYBERSECURITY INCIDENT INFORMATION

A. (U//FOUO) If directed by participating critical infrastructure entities, CenturyLink may provide the U.S. Government, through DHS, information about cybersecurity incidents or attempted cybersecurity incidents involving participating DIB companies that were detected or prevented through cybersecurity services provided in accordance this Agreement sufficient to identify the fact of a particular incident or attempted incident, including, where relevant—
   1. Number of hits per Signature ID within a given time period;
   2. Number of hits per signature per customer (name redacted, unless otherwise agreed by customers) per given time period;
   3. Source IP address for (1) and (2) above;
   4. Number of unique recipients (no names or e-mail addresses) per signature ID per company per given time period;
   5. Whether a link or attachment was included in the e-mail and if the attachment, the attachment type; and,
   6. Specific to DNS redirection, the destination port and protocol and DNS record type for the DNS request.

B. (U//FOUO) For cybersecurity incidents involving U.S. Government agencies, CenturyLink shall provide DHS with additional cybersecurity incident information requested by DHS to support analysis and incident response in accordance with permission provided by such U.S. Government agencies.

C. (U//FOUO) DHS shall only use cybersecurity incident information provided by CenturyLink under this section for cybersecurity purposes in furtherance of its lawful mission.

D. (U) Further dissemination of cybersecurity incident information by DHS shall be limited to U.S. Government entities with primary cybersecurity responsibilities, including employees, contractors, and consultants of those entities having a need to know and have entered into nondisclosure agreements with the U.S. Government. Threat information provided to DHS by CenturyLink on behalf of their customers will be handled and, when appropriate, shared by DHS in

accordance with existing procedures regarding the minimization and anonymization of information not necessary to understand a cyber threat.

E. (U//FOUO) Nothing in this section shall prohibit DHS from using or disseminating cyber threat indicators, including Internet protocol addresses or domain names, derived from cybersecurity incident information as long as such indicators do not identify the source of such information and are not otherwise attributable to CenturyLink or any participating critical infrastructure entity or U.S. Government agency.

F. (U//FOUO) Cybersecurity incident information will be protected from disclosure under the Freedom of Information Act to the maximum extent permitted by law.

G. (U//FOUO) The acceptance by DHS of cybersecurity incident information shall not impact any rights in such information to which the U.S. Government is otherwise entitled or impair the U.S. Government's right to use similar or identical information acquired from other sources

IV. GENERAL PROVISIONS

A. (U//FOUO) This agreement does not promise present or future obligation of funds by the parties.

B. (U//FOUO)The existence of the Agreement and the activities to be conducted under it are intended to further efforts to use GFI to protect critical infrastructure entities and U.S. Government agencies and are not an endorsement of or approval by the Government of CenturyLink, or any of its products or services.

C. (U) Participation in the activities under this Agreement is at the sole discretion of CenturyLink.

D. (U//FOUO) The information provided by the parties under this Agreement is provided without any guarantee, warranty, or assurance of its accuracy or effectiveness, whether express or implied, and the parties assume no liability for use of or reliance on information disclosed under this Agreement.

E. (U//FOUO) DHS authorizes, on behalf of the U.S. Government, use of the GFI provided under this Agreement by CenturyLink for the purposes described herein. If CenturyLink desires to obtain additional rights in such information beyond those needed for activities under Agreement, the parties will enter into good faith negotiations for any required license in accordance with federal law.

F. (U//FOUO) The parties will conduct their respective activities under this Agreement in accordance with applicable laws, including restrictions on the interception, monitoring, access, use, or sharing of electronic communications.

V. POINTS OF CONTACT

A. (U//FOUO) DHS of Homeland Security point of contact is:

Roberta G. Stempfley
Deputy Assistant Secretary
Department of Homeland Security,
Office of Cybersecurity & Communications
703-235-5511

B. (U//FOUO) The CenturyLink point of contact is:

(b) (6)
CenturyLink-Government
(b) (6)

VI. (U) TERMINATION REVIEW

A. (U//FOUO) The parties reserve the right to unilaterally limit, discontinue, or terminate the activities under this Agreement upon written notice by either party.

B. Prior to termination, CenturyLink shall return to DHS or, at DHS's option, destroy all GFI provided to it by DHS and all classified information in CenturyLink's possession as a result of this Agreement, except for the Memorandum of Agreement, appendices thereto, and any associated written approvals thereunder.

C. Termination is the sole remedy under this Agreement for violation of its term and conditions; however, the rights and remedies of the parties that arise from any other source are not limited or affected by this Agreement. Neither party waives any right it may have as a matter of law or contract.

D. Termination of this Agreement does not relieve the parties of the obligation to protect against unauthorized disclosure any information received under this Agreement.

(b) (6)

Name
Title

Date

(b) (6)

Name SVP + GM
Title

1/24/2012
Date

(b) (6)

1/25/2012

Roberta G Stempfley
Deputy Assistant Secretary
Cyber Security and Communications