

FRANK R. WOLF
10TH DISTRICT, VIRGINIA



241 CANNON HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-4610
(202) 225-5136

COMMITTEE ON APPROPRIATIONS

SUBCOMMITTEES:

RANKING MEMBER—STATE-FOREIGN
OPERATIONS

TRANSPORTATION-HUD

CO-CHAIR—CONGRESSIONAL
HUMAN RIGHTS CAUCUS

13873 PARK CENTER ROAD
SUITE 130
HERNDON, VA 20171
(703) 709-5800
(800) 945-9653 (IN STATE)

110 NORTH CAMERON STREET
WINCHESTER, VA 22601
(540) 667-0990
(800) 850-3483 (IN STATE)

Congress of the United States

House of Representatives

January 5, 2009

wolf.house.gov

The Honorable Nancy Pelosi
Speaker of the House
H 232 The Capitol

Dear Madam Speaker:

Last Congress, I introduced a privileged resolution, H. Res. 1263, calling for greater protection of congressional computer and information systems after several computers in my Washington office were compromised by a source within the People's Republic of China. We subsequently learned that computers in the offices of many other Members were similarly compromised, as well as those of the House Foreign Affairs Committee. It is logical to assume that critical and sensitive information about U.S. foreign policy and the work of Congress was open to view from these official computers.

Although my resolution was not acted upon, I received repeated assurances that the issue would be seriously considered and that the leadership of this chamber would take the necessary actions to inform Members about the threats to our computer systems and personal electronic devices – both at home and abroad. Although the Republican Conference and Democratic Caucus held classified briefings for Members in September 2008, the meetings were sparsely attended. I fear that Members are no better informed today than they were before.

I have concluded that only a House rule requiring a mandatory bipartisan briefing on cybersecurity threats to the Congress will be effective in raising awareness of this growing threat. I propose the following rule, or language to similar effect, be included in the rules package to be adopted tomorrow during our first meeting of the 111th Congress:

Rule 1: The Speaker

Sec. 9: Other Responsibilities

The Speaker, in consultation with the Minority Leader, shall arrange for a secret session to be held in the House Chamber on the topic of cybersecurity within the first fifty (50) legislative days of the Congress.

The briefing shall be led by the Sergeant-at-Arms and shall address: (1) threats to House information security, (2) threats to information security when Members travel abroad, and (3) measures being taken secure House computer networks and electronic devices.

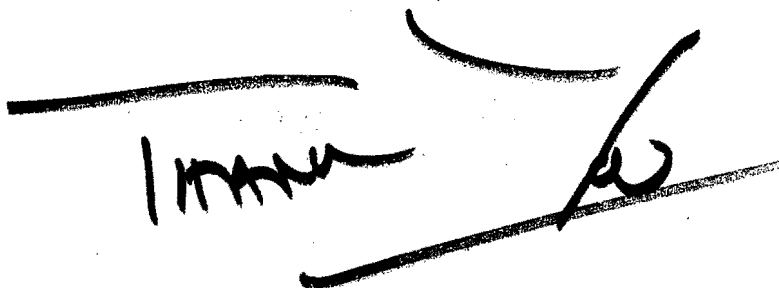
Thank you for your serious consideration. Please do not hesitate to contact me at 5-5136 if I may be of assistance in the implementation of this rule.

Best wishes.

Sincerely,

Frank R. Wolf
Member of Congress

FRW:tc

A large, stylized handwritten signature in black ink, appearing to read 'Frank R. Wolf', is written over the typed name. The signature is highly cursive and loops around the typed text.

FRANK R. WOLF

10TH DISTRICT, VIRGINIA

COMMITTEE ON APPROPRIATIONS

SUBCOMMITTEES:

RANKING MEMBER—STATE-FOREIGN
OPERATIONS

TRANSPORTATION-HUD

CO-CHAIR—CONGRESSIONAL
HUMAN RIGHTS CAUCUS



Congress of the United States
House of Representatives

January 5, 2009

241 CANNON HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-4610
(202) 225-5136

13873 PARK CENTER ROAD
SUITE 130
HERNDON, VA 20171
(703) 709-5800
(800) 945-9653 (IN STATE)

110 NORTH CAMERON STREET
WINCHESTER, VA 22601
(540) 667-0990
(800) 850-3463 (IN STATE)

wolf.house.gov

The Honorable Steny Hoyer
1705 Longworth House Office Building
Washington, DC 20515

Dear 

Last Congress, I introduced a privileged resolution, H. Res. 1263, calling for greater protection of congressional computer and information systems after several computers in my Washington office were compromised by a source within the People's Republic of China. We subsequently learned that computers in the offices of many other Members were similarly compromised, as well as those of the House Foreign Affairs Committee. It is logical to assume that critical and sensitive information about U.S. foreign policy and the work of Congress was open to view from these official computers.

Although my resolution was not acted upon, I received repeated assurances that the issue would be seriously considered and that the leadership of this chamber would take the necessary actions to inform Members about the threats to our computer systems and personal electronic devices – both at home and abroad. Although the Republican Conference and Democratic Caucus held classified briefings for Members in September 2008, the meetings were sparsely attended. I fear that Members are no better informed today than they were before.

I have concluded that only a House rule requiring a mandatory bipartisan briefing on cybersecurity threats to the Congress will be effective in raising awareness of this growing threat. I propose the following rule, or language to similar effect, be included in the rules package to be adopted tomorrow during our first meeting of the 111th Congress:

Rule 1: The Speaker

Sec. 9: Other Responsibilities

The Speaker, in consultation with the Minority Leader, shall arrange for a secret session to be held in the House Chamber on the topic of cybersecurity within the first fifty (50) legislative days of the Congress.

The briefing shall be led by the Sergeant-at-Arms and shall address: (1) threats to House information security, (2) threats to information security when Members travel abroad, and (3) measures being taken secure House computer networks and electronic devices.

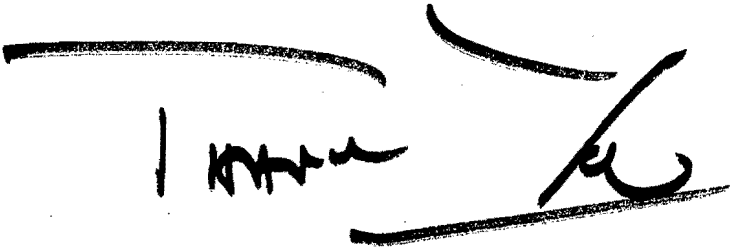
Thank you for your serious consideration. Please do not hesitate to contact me at 5-5136 if I may be of assistance in the implementation of this rule.

Best wishes.

Sincerely,

Frank R. Wolf
Member of Congress

FRW:tc

A large, stylized handwritten signature in black ink, appearing to read 'Frank R. Wolf', is written over the typed name. The signature is composed of several thick, sweeping strokes.

FRANK R. WOLF
10TH DISTRICT, VIRGINIA

COMMITTEE ON APPROPRIATIONS

SUBCOMMITTEES:

RANKING MEMBER—STATE-FOREIGN
OPERATIONS

TRANSPORTATION-HUD

CO-CHAIR—CONGRESSIONAL
HUMAN RIGHTS CAUCUS



Congress of the United States
House of Representatives

January 5, 2009

241 CANNON HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-4610
(202) 225-5136

13873 PARK CENTER ROAD
SUITE 130
HERNDON, VA 20171
(703) 709-5800
(800) 945-9653 (IN STATE)

110 NORTH CAMERON STREET
WINCHESTER, VA 22601
(540) 667-0990
(800) 850-3463 (IN STATE)

wolf.house.gov

The Honorable Louise M. Slaughter
Chairwoman, Committee on Rules
H-312 The Capitol
Washington, DC 20515

Dear Louise

Last Congress, I introduced a privileged resolution, H. Res. 1263, calling for greater protection of congressional computer and information systems after several computers in my Washington office were compromised by a source within the People's Republic of China. We subsequently learned that computers in the offices of many other Members were similarly compromised, as well as those of the House Foreign Affairs Committee. It is logical to assume that critical and sensitive information about U.S. foreign policy and the work of Congress was open to view from these official computers.

Although my resolution was not acted upon, I received repeated assurances that the issue would be seriously considered and that the leadership of this chamber would take the necessary actions to inform Members about the threats to our computer systems and personal electronic devices – both at home and abroad. Although the Republican Conference and Democratic Caucus held classified briefings for Members in September 2008, the meetings were sparsely attended. I fear that Members are no better informed today than they were before.

I have concluded that only a House rule requiring a mandatory bipartisan briefing on cybersecurity threats to the Congress will be effective in raising awareness of this growing threat. I propose the following rule, or language to similar effect, be included in the rules package to be adopted tomorrow during our first meeting of the 111th Congress:

Rule 1: The Speaker

Sec. 9: Other Responsibilities

The Speaker, in consultation with the Minority Leader, shall arrange for a secret session to be held in the House Chamber on the topic of cybersecurity within the first fifty (50) legislative days of the Congress.

The briefing shall be led by the Sergeant-at-Arms and shall address: (1) threats to House information security, (2) threats to information security when Members travel abroad, and (3) measures being taken secure House computer networks and electronic devices.

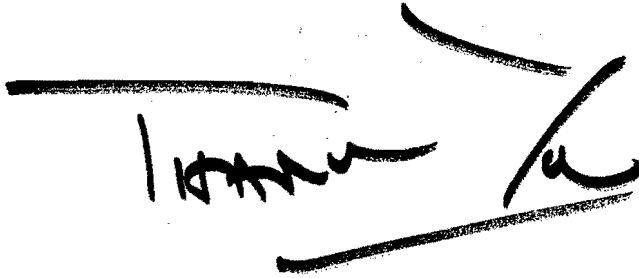
Thank you for your serious consideration. Please do not hesitate to contact me at 5-5136 if I may be of assistance in the implementation of this rule.

Best wishes.

Sincerely,

Frank R. Wolf
Member of Congress

FRW:tc

A handwritten signature in black ink, appearing to read 'Frank R. Wolf', is written below the typed name. The signature is stylized and includes a large flourish at the end.

FRANK R. WOLF

10TH DISTRICT, VIRGINIA

COMMITTEE ON APPROPRIATIONS

SUBCOMMITTEES:

RANKING MEMBER—STATE-FOREIGN
OPERATIONS

TRANSPORTATION-HUD

CO-CHAIR—CONGRESSIONAL
HUMAN RIGHTS CAUCUS



Congress of the United States
House of Representatives

January 5, 2009

241 CANNON HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-4610
(202) 225-5136

13873 PARK CENTER ROAD
SUITE 130
HERNDON, VA 20171
(703) 709-5800
(800) 945-9653 (IN STATE)

110 NORTH CAMERON STREET
WINCHESTER, VA 22601
(540) 667-0990
(800) 850-3463 (IN STATE)

wolf.house.gov

The Honorable John A. Boehner
Minority Leader
U.S. House of Representatives
H204 The Capitol

Dear John:

Last Congress, I introduced a privileged resolution, H. Res. 1263, calling for greater protection of congressional computer and information systems after several computers in my Washington office were compromised by a source within the People's Republic of China. We subsequently learned that computers in the offices of many other Members were similarly compromised, as well as those of the House Foreign Affairs Committee. It is logical to assume that critical and sensitive information about U.S. foreign policy and the work of Congress was open to view from these official computers.

Although my resolution was not acted upon, I received repeated assurances that the issue would be seriously considered and that the leadership of this chamber would take the necessary actions to inform Members about the threats to our computer systems and personal electronic devices – both at home and abroad. Although the Republican Conference and Democratic Caucus held classified briefings for Members in September 2008, the meetings were sparsely attended. I fear that Members are no better informed today than they were before.

I have concluded that only a House rule requiring a mandatory bipartisan briefing on cybersecurity threats to the Congress will be effective in raising awareness of this growing threat. I propose the following rule, or language to similar effect, be included in the rules package to be adopted tomorrow during our first meeting of the 111th Congress:

Rule 1: The Speaker

Sec. 9: Other Responsibilities

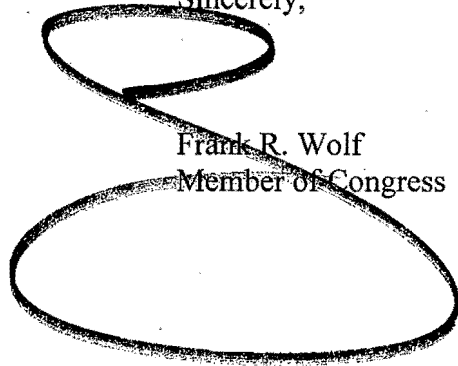
The Speaker, in consultation with the Minority Leader, shall arrange for a secret session to be held in the House Chamber on the topic of cybersecurity within the first fifty (50) legislative days of the Congress.

The briefing shall be led by the Sergeant-at-Arms and shall address: (1) threats to House information security, (2) threats to information security when Members travel abroad, and (3) measures being taken secure House computer networks and electronic devices.

Thank you for your serious consideration. Please do not hesitate to contact me at 5-5136 if I may be of assistance in the implementation of this rule.

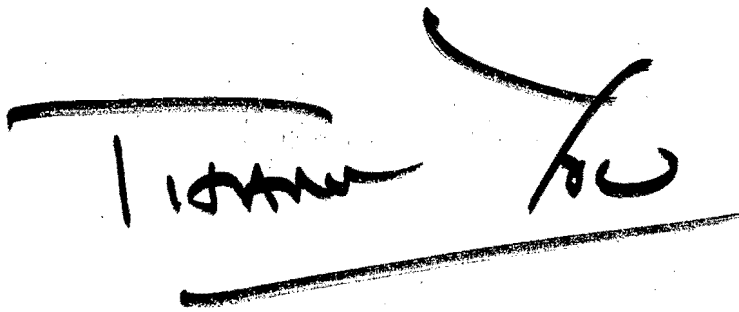
Best wishes.

Sincerely,

A large, stylized handwritten signature in black ink, consisting of a large loop at the top and a larger loop at the bottom.

Frank R. Wolf
Member of Congress

FRW:tc

A handwritten signature in black ink, appearing to read "Tom T. C." with a horizontal line underneath.

FRANK R. WOLF
10TH DISTRICT, VIRGINIA

COMMITTEE ON APPROPRIATIONS

SUBCOMMITTEES:

RANKING MEMBER—STATE-FOREIGN
OPERATIONS

TRANSPORTATION-HUD

CO-CHAIR—CONGRESSIONAL
HUMAN RIGHTS CAUCUS



Congress of the United States
House of Representatives

January 5, 2009

241 CANNON HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-4610
(202) 225-5136

13873 PARK CENTER ROAD
SUITE 130
HERNDON, VA 20171
(703) 709-5800
(800) 945-9653 (IN STATE)

110 NORTH CAMERON STREET
WINCHESTER, VA 22601
(540) 667-0990
(800) 850-3463 (IN STATE)

wolf.house.gov

The Honorable David Dreier
Ranking Member, Committee on Rules
233 Cannon House Office Building
Washington, DC 20515

Dear David:

Last Congress, I introduced a privileged resolution, H. Res. 1263, calling for greater protection of congressional computer and information systems after several computers in my Washington office were compromised by a source within the People's Republic of China. We subsequently learned that computers in the offices of many other Members were similarly compromised, as well as those of the House Foreign Affairs Committee. It is logical to assume that critical and sensitive information about U.S. foreign policy and the work of Congress was open to view from these official computers.

Although my resolution was not acted upon, I received repeated assurances that the issue would be seriously considered and that the leadership of this chamber would take the necessary actions to inform Members about the threats to our computer systems and personal electronic devices – both at home and abroad. Although the Republican Conference and Democratic Caucus held classified briefings for Members in September 2008, the meetings were sparsely attended. I fear that Members are no better informed today than they were before.

I have concluded that only a House rule requiring a mandatory bipartisan briefing on cybersecurity threats to the Congress will be effective in raising awareness of this growing threat. I propose the following rule, or language to similar effect, be included in the rules package to be adopted tomorrow during our first meeting of the 111th Congress:

Rule 1: The Speaker

Sec. 9: Other Responsibilities

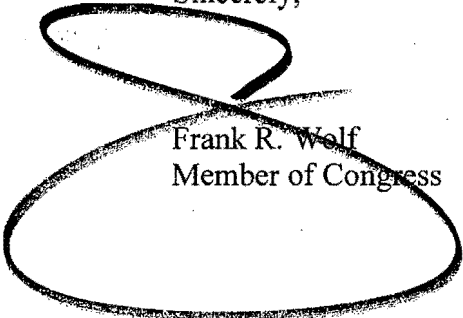
The Speaker, in consultation with the Minority Leader, shall arrange for a secret session to be held in the House Chamber on the topic of cybersecurity within the first fifty (50) legislative days of the Congress.

The briefing shall be led by the Sergeant-at-Arms and shall address: (1) threats to House information security, (2) threats to information security when Members travel abroad, and (3) measures being taken secure House computer networks and electronic devices.

Thank you for your serious consideration. Please do not hesitate to contact me at 5-5136 if I may be of assistance in the implementation of this rule.

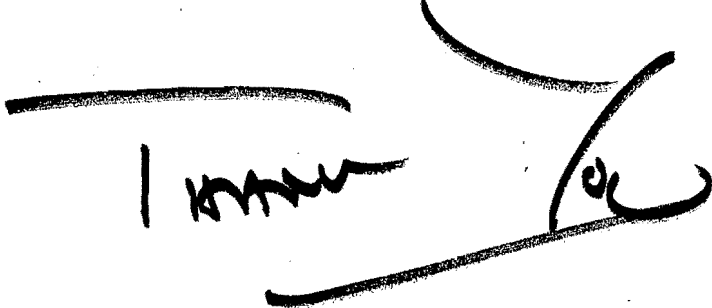
Best wishes.

Sincerely,

A large, stylized handwritten signature in black ink, consisting of several loops and a long horizontal stroke at the bottom.

Frank R. Wolf
Member of Congress

FRW:tc

A handwritten signature in black ink, featuring a horizontal line at the top, a cursive-style name, and a long horizontal stroke at the bottom.