

ALASKA LEGISLATURE COMMITTEE FILES

1999-2000 8672

9952 HOUSE LABOR & COMMERCE

1 soon as permitted by this chapter.

2 \* Sec. 30. AS 21.79.070(h) is amended to read:

3 (h) If the maximum [A ONE PERCENT] assessment for a subaccount of the  
4 life and annuity account in any one year does not provide an amount sufficient to carry  
5 out the responsibilities of the association, the board shall, as provided under (d) of this  
6 section, access [ASSESS] all subaccounts of the life and annuity account for the  
7 necessary additional amount, subject to the assessment limit provided in (f) of this  
8 section.

9 \* Sec. 31. AS 21.79.070 is amended by adding new subsections to read:

10 (i) Assessments for funds to meet the requirements of the association with  
11 respect to an impaired or insolvent insurer may not be authorized or called until  
12 necessary to implement the purposes of this chapter. Classification of assessments  
13 under (b) of this section and computation of assessments under this section shall be  
14 made with a reasonable degree of accuracy, recognizing that exact determinations may  
15 not always be possible. The association shall notify each member insurer of its  
16 anticipated pro rata share of an authorized assessment not yet called within 180 days  
17 after the assessment is authorized.

18 (j) The board may, by an equitable method as established in the plan of  
19 operation, refund to member insurers, in proportion to the contribution of each insurer  
20 to that account, the amount by which the assets of the account exceed the amount the  
21 board finds is necessary to carry out during the coming year the obligations of the  
22 association with regard to that account, including assets accruing from assignment,  
23 subrogation, net realized gains, and income from investments. A reasonable amount  
24 may be retained in any account to provide funds for the continuing expenses of the  
25 association and for future losses claims.

26 (k) A member insurer may, in determining its premium rates and policy owner  
27 dividends as to any kind of insurance within the scope of this chapter, consider the  
28 amount reasonably necessary to meet its assessment obligations under this chapter.

29 (l) A member insurer that wishes to protest all or part of an assessment shall  
30 pay when due the full amount of the assessment as set out in the notice provided by  
31 the association. The payment shall be available to meet association obligations during

1 the pendency of the protest or any subsequent appeal. If a payment is made under  
2 protest, payment must be accompanied by a statement in writing that the payment is  
3 made under protest and setting out a brief statement of the grounds for the protest.  
4 Within 60 days following the payment of an assessment under protest by a member  
5 insurer, the association shall notify the member insurer in writing of its determination  
6 with respect to the protest unless the association notifies the member insurer that  
7 additional time is required to resolve the issues raised by the protest. Within 30 days  
8 after a final decision has been made, the association shall notify the protesting member  
9 insurer in writing of that final decision. Within 60 days of receipt of notice of the  
10 final decision, the protesting member insurer may appeal that final action to the  
11 director. In the alternative to rendering a final decision with respect to a protest based  
12 on a question regarding the assessment base, the association may refer protests to the  
13 director for a final decision with or without recommendation from the association. If  
14 a protest or appeal on an assessment is upheld, the amount paid in error or excess shall  
15 be returned to the member company. Interest on a refund due a protesting member  
16 shall be paid at the rate actually earned by the association.

17 \* Sec. 32. AS 21.79.080(a) is amended to read:

18 (a) The association shall submit to the director a plan of operation and any  
19 amendments to assure the fair, reasonable, and equitable administration of the  
20 association. The plan of operation and any amendments take effect on the written  
21 approval of the plan by the director or 30 days after receipt by the director if not  
22 disapproved by the director.

23 \* Sec. 33. AS 21.79.080(b) is amended to read:

24 (b) If [NOTWITHSTANDING (a) OF THIS SECTION, IF THE  
25 ASSOCIATION FAILS TO SUBMIT A PLAN OF OPERATION ACCEPTABLE TO  
26 THE DIRECTOR BY JULY 1, 1991, OR IF AT A LATER TIME] the association  
27 fails to submit suitable amendments to the plan, the director shall, after notice and  
28 hearing, adopt regulations to implement this chapter. These regulations remain in  
29 effect until amended or repealed by the director [OR SUPERSEDED BY A PLAN  
30 SUBMITTED BY THE ASSOCIATION THAT IS APPROVED BY THE  
31 DIRECTOR].

1 \* Sec. 34. AS 21.79.080(c) is amended to read:

2 (c) A member insurer shall comply with the plan of operation. The plan of  
3 operation must

4 (1) establish procedures for handling assets of the association;

5 (2) establish the amount and method of reimbursing members of the  
6 board under AS 21.79.050(c);

7 (3) establish regular places and times for meetings of the board in the  
8 state; the board may conduct meetings telephonically;

9 (4) establish procedures for keeping records of all financial transactions  
10 of the association, its agents, and the board;

11 (5) establish terms of office for members of the board, and establish  
12 procedures for the selection of the members of the board and for the director's approval  
13 of the members selected;

14 (6) establish additional procedures for assessments under AS 21.79.070;  
15 and

16 (7) contain additional provisions necessary or proper for the association  
17 to exercise its powers and duties.

18 \* Sec. 35. AS 21.79.100(f) is amended to read:

19 (f) The board may [SHALL]

20 (1) make reports and recommendations to the director relating to the  
21 solvency, liquidation, rehabilitation, or conservation of a member insurer or the  
22 solvency of insurers who apply to transact insurance business in the state; the director  
23 and the board shall keep the reports and recommendations confidential;

24 (2) notify the director of any information that indicates that a member  
25 insurer may be impaired or insolvent.

26 \* Sec. 36. AS 21.79.110(b) is amended to read:

27 (b) The association shall keep records of [NEGOTIATIONS AND] meetings  
28 relating to its activities. Records of [NEGOTIATIONS OR] meetings may only be  
29 made public under AS 21.79.040(b)

30 (1) after the termination of a liquidation, rehabilitation, or conservation  
31 proceeding that involves the impaired or insolvent insurer;

1 (2) after the insurer is no longer impaired or insolvent; or

2 (3) upon the order of a court of competent jurisdiction.

3 \* Sec. 37. AS 21.79.110(c) is amended to read:

4 (c) The association is considered to be a creditor of the impaired or insolvent  
5 insurer to the extent of assets attributable to covered policies that are reduced by an  
6 amount to which the association is entitled under AS 21.79.060(s). Assets of the  
7 impaired or insolvent insurer that are attributable to covered policies shall be used to  
8 continue all covered policies and pay all contractual obligations of the impaired or  
9 insolvent insurer as required by this chapter. Assets attributable to covered policies  
10 include those assets that should have been established as reserves for the covered  
11 policies. These assets are determined by multiplying the total assets of the impaired  
12 or insolvent insurer by a fraction, the numerator of which is the amount that should  
13 have been established as reserves for the covered policies of the impaired or insolvent  
14 insurer, and the denominator of which is the amount that should have been established  
15 as reserves for all policies of insurance issued in all states by that insurer. As a  
16 creditor of the impaired or insolvent insurer, the association and other similar  
17 entities in other states are entitled to receive a disbursement of assets out of the  
18 marshaled assets as a credit against contractual obligations under this chapter  
19 from time to time as the assets become available. If the liquidator has not, within  
20 120 days of the date of a final determination of insolvency of an insurer by the  
21 court, made an application to the court for the approval of a proposal to disburse  
22 assets, the association may make application to the court for the approval of the  
23 association's proposal to disburse assets.

24 \* Sec. 38. AS 21.79.110 is amended by adding new subsections to read:

25 (f) A deposit in this state, held by law or required by the director for the  
26 benefit of creditors, including policy owners, not turned over to the domiciliary  
27 liquidator upon the entry of a final order of liquidation or order approving a  
28 rehabilitation plan of an insurer domiciled in this state or in a reciprocal state shall  
29 be promptly paid to the association. The association

30 (1) is entitled to retain a portion of any amount paid to it equal to the  
31 percentage determined by dividing the aggregate amount of policy owners' claims

1 related to that insolvency for which the association has provided statutory benefits by  
2 the aggregate amount of all policy owners' claims in this state related to that  
3 insolvency; and

4 (2) shall remit to the domiciliary receiver the amount paid to the  
5 association and retained under (1) of this subsection; any amount paid to the  
6 association not retained by it under (1) of this subsection shall be treated as a  
7 distribution of state assets under AS 21.78.294 or a similar provision of the state of  
8 domicile of the impaired or insolvent insurer.

9 (g) The association may not be required to give an appeal bond in an appeal  
10 of a civil action arising under this chapter.

11 \* Sec. 39. AS 21.79.120 is amended to read:

12 **Sec. 21.79.120. Examination of the association, annual report.** The  
13 association may be examined by the director. The board shall submit to the director,  
14 not later than July [MAY] 1 of each year, a certified financial report for the preceding  
15 calendar year in a form approved by the director and a report of its activities during  
16 the preceding calendar year. Nothing in AS 21.79.110(b) limits the duty of the  
17 association to report under this section. Upon request, the association shall provide  
18 a copy of the report to a member insurer.

19 \* Sec. 40. AS 21.79.140 is amended to read:

20 **Sec. 21.79.140. Civil immunity.** The association and its agents and  
21 employees, members of the Board of Governors, member insurers, and agents and  
22 employees of member insurers, and the director and the director's representatives are  
23 not civilly liable for an action or omission in performing [TAKEN BY THEM TO  
24 PERFORM] duties under this chapter. In this section, "duties" includes  
25 participation in an organization of one or more state associations of life or health  
26 insurers.

27 \* Sec. 41. AS 21.79.150 is repealed and reenacted to read:

28 **Sec. 21.79.150. Stay of proceedings; default judgment.** Proceedings  
29 involving an insolvent insurer shall be stayed at least 60 days after the date of a final  
30 order of liquidation, rehabilitation, or conservation in order to allow the association to  
31 exercise a power or duty authorized under this chapter. If a default judgment is

1 entered against an insolvent insurer, the association may apply to have the judgment  
2 set aside or may defend against the action on its merits.

3 \* **Sec. 42.** AS 21.79 is amended by adding new sections to read:

4 **Sec. 21.79.160. Prohibited advertisement of insurance sales; required**  
5 **notice.** (a) A person, including an insurer, agent, or affiliate of an insurer, may not  
6 make, publish, disseminate, circulate, or place before the public, or cause, directly or  
7 indirectly, to be made, published, disseminated, circulated, or placed before the public,  
8 in any newspaper, magazine, or other publication, or in the form of a notice, circular,  
9 pamphlet, letter, or poster, or over any radio station or television station, or in any  
10 other way, an advertisement, announcement, or statement, written or oral, that uses the  
11 existence of the association for the purpose of sales, solicitation, or inducement to  
12 purchase any form of insurance covered by the association. However, this section does  
13 not apply to the association or any other entity that does not sell or solicit insurance.

14 (b) The association shall prepare a summary document describing the general  
15 purposes and current limitations of this chapter and complying with (c) of this section.  
16 This document shall be submitted to the director for approval. Beginning 60 days after  
17 the date on which the director approves the document, an insurer may not deliver a  
18 policy or contract to a policy or contract owner unless the summary document is  
19 delivered to the policy or contract owner at the time of delivery of the policy or  
20 contract. The document shall also be available upon request by a policy owner. The  
21 distribution, delivery, contents, or interpretation of this document does not guarantee  
22 that either the policy or the contract, or the owner of the policy or contract, is covered  
23 in the event of the impairment or insolvency of a member insurer. The description  
24 document shall be revised by the association as amendments to this chapter may  
25 require. Failure to receive this document does not give the policy owner, contract  
26 owner, certificate holder, or insured any greater rights than those stated in this chapter.

27 (c) The document prepared under (b) of this section must contain a clear and  
28 conspicuous disclaimer on its face. The director shall establish the form and content  
29 of the disclaimer. The disclaimer must

30 (1) state the name and address of the association and the division of  
31 insurance;

1 (2) prominently warn the policy or contract owner that the association  
2 may not cover the policy or, if coverage is available, that the policy will be subject to  
3 substantial limitations and exclusions and conditioned on continued residence in this  
4 state;

5 (3) state the types of policies for which guaranty funds will provide  
6 coverage;

7 (4) state that the insurer and its agents are prohibited by law from using  
8 the existence of the association for the purpose of sales, solicitation, or inducement to  
9 purchase any form of insurance;

10 (5) state that the policy or contract owner should not rely on coverage  
11 under the association when selecting an insurer;

12 (6) explain rights available and procedures for filing a complaint to  
13 allege a violation of a provision of this chapter; and

14 (7) provide other information as required by the director, including  
15 sources for information about the financial condition of insurers if the information is  
16 not proprietary and is subject by law to disclosure.

17 (d) A member insurer shall retain evidence of compliance with (b) of this  
18 section for so long as the policy or contract for which the notice is given remains in  
19 effect.

20 **Sec. 21.79.170. Determination of principal place of business.** (a) Except  
21 as provided under (b) of this section, the principal place of business of a plan sponsor  
22 or a person other than a natural person is that state in which the plan sponsor or person  
23 exercises the direction, control, and coordination of the operations of the entity, as  
24 determined by the association in its reasonable judgment by considering the following  
25 factors:

26 (1) the state in which the primary executive and administrative  
27 headquarters of the entity are located;

28 (2) the state in which the principal office of the chief executive officer  
29 of the entity is located;

30 (3) the state in which the board of directors or a similar governing body  
31 of the entity conducts the majority of its meetings;

1 (4) the state in which the executive or management committee of the  
2 board of directors or a similar governing body of the entity conducts the majority of  
3 its meetings;

4 (5) the state from which the management of the overall operations of  
5 the entity is directed; and

6 (6) in the case of a benefit plan sponsored by affiliated companies  
7 making up a consolidated corporation, the state in which the holding company or  
8 controlling affiliate has its principal place of business as determined using the factors  
9 described in this subsection.

10 (b) In the case of a plan sponsor, if more than 50 percent of the participants  
11 in the benefit plan are employed in a single state, that state is the principal place of  
12 business of the plan sponsor.

13 **Sec. 21.79.180. Determination of residency of certain individuals.** A citizen  
14 of the United States that is either a (1) resident of a foreign country, or (2) resident of  
15 a United States possession, territory, or protectorate that does not have an association  
16 similar to the association created by this chapter is, for purposes of this chapter, a  
17 resident of the state of domicile of the insurer that issued the policy or contract.

18 \* **Sec. 43.** AS 21.79.900(6) is amended to read:

19 (6) "member insurer" means an insurer licensed to transact insurance  
20 in the state that issues a policy described in AS 21.79.020(a) and (b), or a subscriber  
21 contract providing benefits described in AS 21.87.120(a)(2) - (4) or 21.87.130(a)(2)  
22 and (3), and includes an insurer whose license or certificate of authority in this state  
23 may have been suspended, revoked, not renewed, or voluntarily withdrawn; "member  
24 insurer" does not include

25 (A) a health maintenance organization licensed under AS 21.86;

26 (B) a fraternal benefit society licensed under AS 21.84;

27 (C) a mandatory state pooling plan;

28 (D) a mutual assessment company or an entity that operates on  
29 an assessment basis;

30 (E) an insurance exchange licensed under AS 21.75; [OR]

31 (F) a [NONPROFIT] hospital or medical service organization

1 licensed under AS 21.87;

2 (G) an organization that has a license or certificate limited  
3 to the issuance of charitable gift annuities; or

4 (H) an entity similar to one described under (A) - (G) of this  
5 paragraph;

6 \* Sec. 44. AS 21.79.900(9) is amended to read:

7 (9) "resident" means a person to whom a contractual obligation is  
8 owed under this chapter and who resides in this state on the date of entry of a  
9 court order that determines a member insurer to be an impaired or insolvent  
10 insurer, whichever occurs first [AT THE TIME A MEMBER INSURER IS  
11 DETERMINED TO BE AN IMPAIRED OR INSOLVENT INSURER AND TO  
12 WHICH A CONTRACTUAL OBLIGATION IS OWED]; a person may be a resident  
13 of only one state, which, in the case of a person other than a natural person, shall be  
14 the principal place of business;

15 \* Sec. 45. AS 21.79.900 is amended by adding new paragraphs to read:

16 (12) "authorized assessment" means an assessment approved by a  
17 resolution by the board that will be called immediately or in the future from member  
18 insurers for a specified amount;

19 (13) "called" means that a notice has been issued by the association to  
20 member insurers requiring that an authorized assessment be paid within the time set  
21 out in the notice;

22 (14) "impaired insurer" means a member insurer that is not an insolvent  
23 insurer and that is placed under an order of rehabilitation or conservation by a court  
24 of competent jurisdiction;

25 (15) "insolvent insurer" means a member insurer that is placed under  
26 an order of liquidation by a court of competent jurisdiction with a finding of  
27 insolvency;

28 (16) "owner," in relation to a policy or contract,

29 (A) means the person who is identified as the legal owner under  
30 the terms of the policy or contract, or who is otherwise vested with legal title  
31 to the policy or contract through a valid assignment completed under the terms

1 of the policy or contract and who is properly recorded as the owner on the  
2 records of the insurer;

3 (B) does not include a person with a mere beneficial interest in  
4 a policy or contract;

5 (17) "plan sponsor" means, in the case of a benefit plan established or  
6 maintained by

7 (A) a single employer, the employer;

8 (B) an employee organization, the employee organization; or

9 (C) two or more employers or jointly by one or more employers  
10 and one or more employee organizations, the association, committee, joint  
11 board of trustees, or other group of representatives of the parties who establish  
12 or maintain the benefit plan;

13 (18) "receivership court" means the court in the insolvent or impaired  
14 insurer's state having jurisdiction over the conservation, rehabilitation, or liquidation  
15 of the insurer;

16 (19) "structured settlement annuity" means an annuity purchased in  
17 order to fund periodic payments for a plaintiff or other claimant in payment for or with  
18 respect to personal injury suffered by the plaintiff or other claimant;

19 (20) "state" means a state of the United States, the District of  
20 Columbia, Puerto Rico, or a United States possession, territory, or protectorate.

21 \* Sec. 46. AS 21.36.035, AS 21.79.060(b), 21.79.100(g), and 21.79.100(i) are repealed.

22 \* Sec. 47. The uncodified law of the State of Alaska is amended by adding a new section  
23 to read:

24 **TRANSITIONAL PROVISIONS.** The terms of the members of the board of governors  
25 of the Alaska Life and Health Insurance Guaranty Association who are serving on the  
26 effective date of this Act are not affected by this Act. Their terms expire as provided before  
27 the enactment of this Act.

(7)

HOUSE COMMITTEE REPORT

Date Referred to Committee: February 16, 2000

FURTHER REFERRALS:

Judiciary

Date of Committee Action: March 3, 2000

The LABOR AND COMMERCE Committee considered:

HB 398

HOUSE BILL NO. 398

LIFE AND HEALTH INSURANCE GUARANTY ASSN

"An Act relating to the Alaska Life and Health Insurance Guaranty Association."

recommends it be replaced with the following committee substitute CS HB 398 (L+C)  the same title  a new title

additional referral to \_\_\_\_\_ Committee  
 attached amendment(s)

ADOPTS: \_\_\_\_\_ Letter of Intent

ATTACHES NEW FISCAL NOTE(S): (Dept) \_\_\_\_\_ APPROVES PREVIOUS: (Dept/Date) \_\_\_\_\_  
 fiscal note(s) \_\_\_\_\_  fiscal note(s) \_\_\_\_\_

zero fiscal note(s) Dced 2/28/00  zero fiscal note(s) \_\_\_\_\_

SIGNING WITH RECOMMENDATIONS	DP	DNP	NR	AM
			<input checked="" type="checkbox"/>	
			<input checked="" type="checkbox"/>	
	<input checked="" type="checkbox"/>			
	<input checked="" type="checkbox"/>			
	<input checked="" type="checkbox"/>			

CHAIR'S SIGNATURE Nann Pokely

3-3-00

**Subject: HB 398 (Life/Health Guaranty Association Bill)**

**Date: Fri, 03 Mar 2000 12:12:50 -0900**

**From: Bob Lohr <Bob\_Lohr@dced.state.ak.us>**

**To: Janet S Seitz <Janet\_Seitz@legis.state.ak.us>**

We have worked closely and productively with the American Council of Life Insurance and John George to settle almost every point of potential disagreement on this bill. We would like to be able to wholeheartedly support HB 398.

There is one potential amendment that concerns us, that would add the right to intervene to Sec. 21. The consensus bill does not contain this phrase and the division does not believe it is needed. Under both the guaranty statute and receivership statute (21.78.100(k)) guaranty associations have standing to appear in court to protect their interests.

Since it involves court proceedings, one option would be to see whether House Judiciary would consider the amendment when they review the bill.



RECEIVED  
FEB 18 2000

ALASKA STATE LEGISLATURE  
REPRESENTATIVE JOHN HARRIS  
STATE CAPITOL 110, JUNEAU, ALASKA 99801-1182 (907) 465-4859

**MEMORANDUM**

February 18, 2000

To: Representative Norman Rokeberg, chairman  
House Committee on Labor and Commerce

From: Representative John Harris 

Re: Request for hearing

Please schedule a committee hearing on HB <sup>3</sup>298 as soon as your calendar will accommodate it. This bill updates the Alaska Life and Health Guaranty Association Act to bring Alaska's law into conformity with the most recent model legislation of the National Association of Insurance Commissioners.

Attached to this memo are a copy of the bill and a sponsor statement. If you need additional information, please contact John Manly of my office.

Thank you for your expeditious attention to this request.



ALASKA STATE LEGISLATURE  
REPRESENTATIVE JOHN HARRIS  
STATE CAPITOL 110, JUNEAU, ALASKA 99801-1182 (907) 465-4859

## Sponsor Statement

### HB 398

"An Act relating to the Alaska Life and Health Insurance Guaranty Association."

The purpose of HB 398 is to make changes to the Alaska Life and Guaranty Association Act (AS 21.79), which provides a mechanism to protect policyholders and claimants in the event of the insolvency of a life and health insurer licensed to sell policies in Alaska.

The Alaska Life and Health Guaranty Association membership is mandatory for every life and health insurer licensed to sell policies in the state. The association, to fund certain outstanding obligations of life and health insurers that have been put into receivership, assesses its members. The Association works closely with the Director of Insurance, who is the receiver for insolvent insurers.

Alaska's current law is based on an earlier version of a national Association of Insurance Commissioners model Act. HB 398 updates Alaska statutes to bring them into close conformity with the most recent National Association of Insurance Commissioners model Act. The NAIC model Act has been updated to reflect lessons learned at a nationwide level from application of the model Act to actual insolvencies experienced since the last revision. HB 398 will allow the Alaska Guaranty Association to better meet its intended purpose of protecting Alaska policyholders and claimants. Updating the Act to comply with the latest model Act provides the added benefit of uniformity among the states in responding to insurer insolvencies.

The Alaska Life and Health Guaranty Association supports passage of HB 398.

# FISCAL NOTE

**STATE OF ALASKA**  
**2000 LEGISLATIVE SESSION**

**BILL NO. HB 398**

Revision Date/Time (Note if correction) \_\_\_\_\_ Dept. Affected Community & Economic Development  
 Title An Act relating to the Alaska Life and Health BRU Insurance  
Insurance Guaranty Association. Component Insurance  
 Sponsor Representative Harris  
 Requester (H) L&C Component No. 354

**Expenditures/Revenues** (Thousands of Dollars)

Note: Amounts do not include inflation unless otherwise noted below.

OPERATING EXPENDITURES	FY 2001	FY 2002	FY 2003	FY 2004	FY 2005	FY 2006
Personal Services						
Travel						
Contractual						
Supplies						
Equipment						
Land & Structures						
Grants & Claims						
Miscellaneous						
<b>TOTAL OPERATING</b>	<b>0.0</b>	<b>0.0</b>	<b>0.0</b>	<b>0.0</b>	<b>0.0</b>	<b>0.0</b>

<b>CAPITAL EXPENDITURES</b>						
-----------------------------	--	--	--	--	--	--

<b>CHANGE IN REVENUES ( )</b>						
-------------------------------	--	--	--	--	--	--

**FUND SOURCE** (Thousands of Dollars)

1002 Federal Receipts						
1003 GF Match						
1004 GF						
1005 GF/Program Receipts						
1037 GF/Mental Health						
Other (Specify Type)						
<b>TOTAL</b>	<b>0.0</b>	<b>0.0</b>	<b>0.0</b>	<b>0.0</b>	<b>0.0</b>	<b>0.0</b>

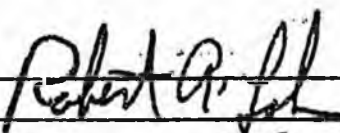
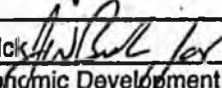
Estimate of any current year (FY2000) cost: 0.0

**POSITIONS**

Full-time						
Part-time						
Temporary						

**ANALYSIS:** (Attach a separate page if necessary)

No fiscal impact on this component.

Prepared by: Robert A. Lohr  Phone 269-7900  
 Division Insurance Date/Time 2-28-00 12:17 PM  
 Approved by Commissioner Deborah B. Sedwick  Date 2-28-00  
 Agency Community & Economic Development

**PREPARER TO PROVIDE ALL DISTRIBUTION COPIES TO GOVERNOR'S LEGISLATIVE OFFICE**

For further distribution information, call the Governor's Legislative Office

**HB**

**401**

(7)

# HOUSE COMMITTEE REPORT

Date Referred to Committee: February 17, 2000

FURTHER REFERRALS:

Judiciary

Date of Committee Action: 24 MAR 2000

The LABOR AND COMMERCE Committee considered:

HB 401

HOUSE BILL NO. 401

COMPUTER NETWORKS AND SPAM ADS

"An Act relating to computer networks and to electronic mail advertisements."

recommends it be replaced  
with the following committee substitute

CSHB 401 (L+C)

the same title  
 a new title

additional referral to \_\_\_\_\_ Committee

attached amendment(s)

ADOPTS: \_\_\_\_\_ Letter of Intent

ATTACHES NEW FISCAL NOTE(S): (Dept)

APPROVES PREVIOUS: (Dept/Date)

fiscal note(s) DOA 3/23/00;  
Corrections 3/22/00; LAW 3/20/00

fiscal note(s) \_\_\_\_\_

zero fiscal note(s) \_\_\_\_\_

zero fiscal note(s) \_\_\_\_\_

SIGNING WITH RECOMMENDATIONS	DP	DN	Ind	AM
<i>Tom Brien</i>			<input checked="" type="checkbox"/>	
<i>John J. Starnes</i>	<input checked="" type="checkbox"/>			
<i>Nancy Kately</i>	<input checked="" type="checkbox"/>			

CHAIR'S SIGNATURE

*Nancy Kately*

3-24-2000

# FISCAL NOTE

STATE OF ALASKA  
2000 LEGISLATIVE SESSION

BILL NO. HB 401

Revision Date/Time (Note if correction) 3/23/00 Dept. Affected Administration  
 Title "An Act relating to computer networks and to BRU Legal and Advocacy Services  
electronic mail advertisements." Component Public Defender Agency  
 Sponsor Representative Rokeberg  
 Requester (H) L&C Component No. 1631

**Expenditures/Revenues** (Thousands of Dollars)

Note: Amounts do not include inflation unless otherwise noted below.

OPERATING EXPENDITURES	FY 2001	FY 2002	FY 2003	FY 2004	FY 2005	FY 2006
Personal Services	.	.	.	.	.	.
Travel						
Contractual						
Supplies						
Equipment						
Land & Structures						
Grants & Claims						
Miscellaneous						
<b>TOTAL OPERATING</b>	.	.	.	.	.	.

CAPITAL EXPENDITURES	.	.	.	.	.	.
----------------------	---	---	---	---	---	---

CHANGE IN REVENUES ( )	.	.	.	.	.	.
------------------------	---	---	---	---	---	---

**FUND SOURCE** (Thousands of Dollars)

1002 Federal Receipts	.	.	.	.	.	.
1003 GF Match						
1004 GF						
1005 GF/Program Receipts						
1037 GF/Mental Health						
Other (Specify Type)						
<b>TOTAL</b>	.	.	.	.	.	.

Estimate of any current year (FY2000) cost: \_\_\_\_\_

**POSITIONS**

Full-time						
Part-time						
Temporary						

**ANALYSIS:** (Attach a separate page if necessary)

See attached.

Prepared by: Barbara Brink, Director Phone 264-4414  
 Division Public Defender Agency Date/Time \_\_\_\_\_  
 Approved by Commissioner -- Robert Poe, Jr. *Arlson M. Elger* Date 3/23/00  
 Agency Department of Administration

**PREPARER TO PROVIDE ALL DISTRIBUTION COPIES TO GOVERNOR'S LEGISLATIVE OFFICE**

For further distribution information, call the Governor's Legislative Office

# FISCAL NOTE

STATE OF ALASKA  
2000 LEGISLATIVE SESSION

BILL NO. HB 401

ANALYSIS CONTINUED:

This bill amends the Criminal Mischief in the First Degree statute. First degree criminal mischief is a class B felony and outlaws such things as intentionally interrupting public utility services and causing over \$100,000 damage to private property by widely dangerous means.

The amendment proposed by this bill would include damaging a computer network that provides service to the public with intent to cause a substantial interruption or impairment of a service rendered to the public in first degree criminal mischief. Also, the definition of "utility" is modified to include Internet Service Providers.

The Public Defender Agency is unable to estimate how many additional cases it would be appointed to if the bill becomes law. It is clear, however, that these will be serious cases. They will also be difficult to defend because these offenses will probably be highly technical in nature. Therefore, although we do anticipate some fiscal impact, we are not able to quantify it and are submitting an indeterminate fiscal note.

**AMENDMENT**

**OFFERED IN THE HOUSE**

**BY REP. ROKEBERG**

**TO: CS HB 401 (), LS 1470\G, Luckhaupt, 3/23/00**

**Page 2, line 24: After "more people"**

**DELETE: "and"**

**INSERT: "or"**

**Page 2, line 30: After "more people"**

**DELETE: "and"**

**INSERT: "or"**

I-LS1470G  
Luckhaupt  
3/23/00

CS FOR HOUSE BILL NO. 401( )

IN THE LEGISLATURE OF THE STATE OF ALASKA

TWENTY-FIRST LEGISLATURE - SECOND SESSION

BY

Offered:  
Referred:

Sponsor(s): REPRESENTATIVE ROKEBERG

A BILL

FOR AN ACT ENTITLED

1 "An Act relating to computer networks and to electronic mail advertisements."

2 BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF ALASKA:

3 \* Section 1. AS 11.46.480(a) is amended to read:

4 (a) A person commits the crime of criminal mischief in the first degree if,  
5 having no right to do so or any reasonable ground to believe the person has such a  
6 right,

7 (1) with intent to cause a substantial interruption or impairment of a  
8 service rendered to the public by a utility or by an organization that [WHICH] deals  
9 with emergencies involving danger to life or property, or rendered to the public by  
10 another person over a computer network, the person damages or tampers with  
11 property of that utility, [OR] organization, or person and causes substantial  
12 interruption or impairment of service to the public;

13 (2) with intent to damage property of another by the use of widely  
14 dangerous means, the person damages property of another in an amount exceeding  
15 \$100,000 by the use of widely dangerous means;

L

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31

(3) the person intentionally damages an oil or gas pipeline or supporting facility; or

(4) with intent to cause physical injury to another person, the person [:]

(A) tampers with an item that is a food, drug, or cosmetic or a container for the item; or

(B) delivers, dispenses, or distributes an item described in (A) of this paragraph knowing that a person has tampered with the item.

\* Sec. 2. AS 11.46.490(7) is amended to read:

(7) "utility" means an enterprise, whether publicly or privately owned or operated, that [WHICH] provides gas, electric, steam, water, sewer, or communications service, and any common carrier; in this paragraph, "communications service" includes Internet service providers and the Internet and its ancillary services;

\* Sec. 3. AS 45.50.471(b) is amended by adding a new paragraph to read:

(43) violating AS 45.50.479 (unsolicited electronic mail advertisements).

\* Sec. 4. AS 45.50 is amended by adding a new section to read:

**Sec. 45.50.479. Provider's restriction on use of electronic mail service. (a)**

A registered user of an electronic mail service may not use or cause to be used the provider's service or equipment in violation of the provider's published policy prohibiting or restricting the use of its service or equipment for the initiation of unsolicited advertisements if the user has previously sent an unsolicited advertisement to 25 or more people and has previously been warned by the provider or recipient for sending unsolicited advertisements.

(b) A person may not, by initiating an unsolicited advertisement, use or cause to be used the service or equipment of an electronic mail service provider in violation of the provider's published policy prohibiting or restricting the use of its service or equipment to deliver unsolicited advertisements if the user has previously sent an unsolicited advertisement to 25 or more people and has previously been warned by the provider or a recipient for sending unsolicited advertisements.

1 (c) This section may not be interpreted to require an electronic mail service  
2 provider to adopt a policy prohibiting or restricting the use of its service or equipment  
3 for the initiation or delivery of unsolicited advertisements. This section does not limit  
4 or restrict the authority of an electronic mail service provider to enforce its policies or  
5 to prohibit or restrict the use of its services or equipment.

6 (d) An electronic mail service provider is considered to have published the  
7 provider's policy on unsolicited advertisements if the provider

8 (1) makes the policy available on request in written form at no charge  
9 to the requester; or

10 (2) displays the policy through an on-line notice on the provider's  
11 Internet home page or on a page accessible through a conspicuous link on the  
12 provider's Internet home page.

13 (e) In this section,

14 (1) "advertisement" means an electronic mail message, the principal  
15 purpose of which is to promote, directly or indirectly, the sale or other distribution of  
16 real property, goods, or services;

17 (2) "electronic mail" means a message or a file that is transmitted  
18 through a local, regional, or global network, regardless of whether the message, file,  
19 or other information is

20 (A) viewed;

21 (B) stored for retrieval at a later time;

22 (C) printed onto paper or other similar material; or

23 (D) filtered or screened by a computer program that is designed  
24 or intended to filter or screen items of electronic mail;

25 (3) "electronic mail service provider" or "provider" means a business  
26 or organization qualified to do business in the state that provides registered users with  
27 the ability to send or receive electronic mail;

28 (4) "initiation" of an unsolicited advertisement refers to the action by  
29 the initial sender of the advertisement; it does not refer to the actions of any  
30 intervening electronic mail service providers that may handle or retransmit the  
31 electronic message;

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11

(5) "network" means a network made up of one or more computers that may be accessed by a modem, electronic or optical technology, or other similar means;

(6) "recipient" means a person who receives an item of electronic mail;

(7) "registered user" means an individual, corporation, or other person that maintains an electronic mail address with an electronic mail service provider;

(8) "unsolicited advertisement" means an electronic mail advertisement that is

(A) addressed to a recipient with whom the initiator does not have an existing business or personal relationship; and

(B) not sent at the request of or with the express consent of the recipient.

# ALASKA STATE LEGISLATURE

## House of Representatives

### COMMITTEE ASSIGNMENTS:

LABOR & COMMERCE COMMITTEE, CHAIRMAN  
JUDICIARY COMMITTEE, MEMBER  
LEGISLATIVE COUNCIL, MEMBER  
SPECIAL COMMITTEE ON UTILITY RESTRUCTURING, MEMBER  
SPECIAL COMMITTEE ON ECONOMIC DEVELOPMENT &  
TOURISM, MEMBER

e-mail: Representative\_Norman\_Rokeberg@legis.state.ak.us



INTERIM:  
716 WEST 4TH AVENUE, SUITE 640  
ANCHORAGE, AK 99501  
PHONE: (907) 269-0117  
FAX: (907) 269-0119

SESSION:  
ALASKA STATE CAPITOL  
JUNEAU, AK 99801-1182  
PHONE: (907) 465-4968  
FAX: (907) 465-2040

## Representative Norman Rokeberg

### SPONSOR STATEMENT HOUSE BILL 401

**An Act relating to computer networks and to electronic mail advertisements  
By Representative Norman Rokeberg**

**HB 401 adds protections for consumers and internet service providers from such things as intentional disruption (e.g., a denial of service attack) or impairment of a service rendered to the public by a utility or emergency organization, or computer network, etc. Such actions would be a crime of criminal mischief in the first degree under HB 401.**

**In the definition of "utility", HB 401 adds language stating that a "communications service" includes Internet service providers and the Internet and its ancillary services.**

**Next HB 401 provides that a user of an e-mail service may not use the provider's service in violation of any published policy of the provider (e.g., anti-spamming provisions). Additionally, the bill provides that the e-mail service provider does not have to adopt a policy prohibiting or restricting use of its services for delivery of unsolicited advertisements – in other words, if the provider wants to adopt a policy, that is fine. "Published" can be by means of written form, or display through on-line notice.**

**As we all move towards greater involvement with e-commerce, consumers need to know that some protections are available to them from such things as unsolicited advertisements. HB 401 would provide this protection.**

**I would urge your support of this legislation.**

**ED 1:03/05/00**

# ALASKA STATE LEGISLATURE

## House of Representatives

### COMMITTEE ASSIGNMENTS:

LABOR & COMMERCE COMMITTEE, CHAIRMAN  
JUDICIARY COMMITTEE, MEMBER  
LEGISLATIVE COUNCIL, MEMBER  
SPECIAL COMMITTEE ON UTILITY RESTRUCTURING, MEMBER  
SPECIAL COMMITTEE ON ECONOMIC DEVELOPMENT &  
TOURISM, MEMBER

e-mail: Representative\_Norman\_Rokeberg@legis.state.ak.us



INTERIM:  
716 WEST 4TH AVENUE, SUITE 640  
ANCHORAGE, AK 99501  
PHONE: (907) 269-0117  
FAX: (907) 269-0119

SESSION:  
ALASKA STATE CAPITOL  
JUNEAU, AK 99801-1182  
PHONE: (907) 465-4968  
FAX: (907) 465-2040

## Representative Norman Rokeberg

### SECTIONAL ANALYSIS

#### HOUSE BILL 401

**An Act relating to computer networks and to electronic mail advertisements**

**By Representative Norman Rokeberg**

**Section 1:** Amends criminal law to provide that it is the crime of criminal mischief in the first degree if a person, having no right to do so, causes substantial interruption or impairment of a service rendered to the public by a utility or organization dealing with emergencies, or rendered to the public by another person over a computer network.

**Section 2:** Amends the definition of "utility" and the subdefinition of "communications service" to include Internet service providers, and the Internet and its ancillary services.

**Section 3:** Adds reference to 45.50.479 to

**Section 4:** Adds new section concerning provider's restriction on use of electronic mail service. Includes description of the provider's policy and how it can be published. Defines "advertisement", "electronic mail", "electronic mail service provider", "provider", "initiation", "network", "recipient", "registered user", and "unsolicited advertisement".

ED 01:03/06/00

# FISCAL NOTE

**STATE OF ALASKA**  
**2000 LEGISLATIVE SESSION**

**BILL NO. HB 401**

Revision Date/Time (Note if correction) _____	Dept. Affected <u>Department of Corrections</u>
Title <u>An Act relating to computer networks and to</u>	BRU <u>Administration and Operations</u>
<u>electronic mail advertisements</u>	Component <u>All</u>
Sponsor <u>Representative Rokeberg</u>	
Requester <u>House Labor and Commerce Committee</u>	Component No. <u>#0694</u>

**Expenditures/Revenues** (Thousands of Dollars)

Note: Amounts do not include inflation unless otherwise noted below.

OPERATING EXPENDITURES	FY 2001	FY 2002	FY 2003	FY 2004	FY 2005	FY 2006
Personal Services						
Travel						
Contractual						
Supplies						
Equipment						
Land & Structures						
Grants & Claims						
Miscellaneous						
<b>TOTAL OPERATING</b>	***	***	***	***	***	***

<b>CAPITAL EXPENDITURES</b>						
-----------------------------	--	--	--	--	--	--

<b>CHANGE IN REVENUES ( )</b>						
-------------------------------	--	--	--	--	--	--

**FUND SOURCE** (Thousands of Dollars)

1002 Federal Receipts						
1003 GF Match						
1004 GF						
1005 GF/Program Receipts						
1037 GF/Mental Health						
Other (Specify Type)						
<b>TOTAL</b>	***	***	***	***	***	***

Estimate of any current year (FY2000) cost: 0.0

**POSITIONS**

Full-time						
Part-time						
Temporary						

**ANALYSIS:** (Attach a separate page if necessary)

See attached analysis.

Prepared by: <u>Candy Brower, Legislative Liaison</u>	Phone <u>465-3307</u>
Division: <u>Commissioner's Office</u>	Date/Time: <u>3/22/00 1:42 PM</u>
Approved by: <u>Commissioner Margaret M. Pugh</u> <i>Margaret M. Pugh</i>	Date: <u>3/22/00</u>
Agency: <u>Dept. of Corrections</u>	

**PREPARER TO PROVIDE ALL DISTRIBUTION COPIES TO GOVERNOR'S LEGISLATIVE OFFICE**

For further distribution information, call the Governor's Legislative Office

**FISCAL NOTE**

**STATE OF ALASKA  
2000 LEGISLATIVE SESSION  
DEPARTMENT OF CORRECTIONS**

**BILL NO. HB 401  
PAGE 2 of 2  
DATE 3/22/00**

**ANALYSIS:**

If passed, this legislation would make it a B Felony (Criminal Mischief I) to intentionally cause a substantial interruption or impairment of a service rendered to the public by another person over a computer network by damaging or tampering with that person's property. This includes the Internet service providers and the Internet and its ancillary services. There has been attention in the media regarding such incidents recently, however, it is difficult to project how often this might occur and whose jurisdiction such an offender would be under. Federal jurisdiction might supersede State jurisdiction in some cases.

While it is the Department of Corrections assumption that these cybercrimes are the wave of the future, and that these offenders are likely to be first time offenders, it is difficult to estimate fiscal impact to the Department. Therefore, the Department of Corrections is submitting an indeterminate fiscal note.

# FISCAL NOTE

STATE OF ALASKA  
2000 LEGISLATIVE SESSION

BILL NO. HB 401

Revision Date/Time (Note if correction) _____	Dept. Affected <u>Law</u>
Title <u>"An Act relating to computer networks and to electronic mail advertisements."</u>	BRU <u>Criminal Division/Civil Division</u>
Sponsor <u>Representative Rokeberg</u>	Component <u>1st-4th Jud Dist; Criminal Appeals/Special Lit/Fair Business Practices</u>
Requester <u>House Labor and Commerce Committee</u>	Component No. <u>2198-99,2201,03,61,79,06</u>

**Expenditures/Revenues** (Thousands of Dollars)

Note: Amounts do not include inflation unless otherwise noted below.

OPERATING EXPENDITURES	FY 2001	FY 2002	FY 2003	FY 2004	FY 2005	FY 2006
Personal Services						
Travel						
Contractual						
Supplies						
Equipment						
Land & Structures						
Grants & Claims						
Miscellaneous						
<b>TOTAL OPERATING</b>	*****	*****	*****	*****	*****	*****

CAPITAL EXPENDITURES						
----------------------	--	--	--	--	--	--

CHANGE IN REVENUES ( )						
------------------------	--	--	--	--	--	--

**FUND SOURCE** (Thousands of Dollars)

FUND SOURCE	FY 2001	FY 2002	FY 2003	FY 2004	FY 2005	FY 2006
1002 Federal Receipts						
1003 GF Match						
1004 GF						
1005 GF/Program Receipts						
1037 GF/Mental Health						
Other (Specify Type)						
<b>TOTAL</b>	*****	*****	*****	*****	*****	*****

Estimate of any current year (FY2000) cost: \_\_\_\_\_

**POSITIONS**

Full-time						
Part-time						
Temporary						

**ANALYSIS:** (Attach a separate page if necessary)

HB 401 makes it a class B felony to intentionally and substantially interrupt or impair a service rendered to the public by another person over a computer network by damaging or tampering with that person's property. In addition, the bill adds to the Unfair Trade Practices and Consumer Protection Act restrictions on the use of a provider's electronic mail service to initiate unsolicited e-mail advertisements.

The Department of Law does not anticipate a fiscal impact on the Consumer Protection unit from the latter change. The addition of a new felony level crime will impact the department; however, it is difficult to quantify what the impact will be. We have no way of estimating how widespread this terroristic conduct is in Alaska, and how often prosecution would fall to state as opposed to federal law enforcement as this type of hacking often crosses state, and national, boundaries.

Prepared by: <u>Joan M. Kasson</u> <i>Joan M. Kasson</i>	Phone <u>465-5370</u>
Division <u>Attorney General's Office</u>	Date/Time <u>3/20/00, 9:09 AM</u>
Approved by <u>Commissioner Kaelin</u> <i>Kaelin</i> <u>Bruce M. Botelho, Attorney General</u>	Date <u>3/20/00</u>
Agency <u>Department of Law</u>	

**PREPARER TO PROVIDE ALL DISTRIBUTION COPIES TO GOVERNOR'S LEGISLATIVE OFFICE**

For further distribution information, call the Governor's Legislative Office

# Hackers increase attacks on Web sites

The Associated Press

NEW YORK—An electronic assault on some of the biggest sites in cyberspace is renewing calls for better high-tech security by businesses and government. But even proponents of stricter measures acknowledged there was no ironclad defense.

Hackers stepped up this week's attack on Wednesday, inconveniencing millions of Internet users and unnerving Wall Street. The apparently coordinated attacks spread to ETrade, ZDNet and other major sites—all of them disturbed by a barrage of messages.

Federal officials urged businesses to install protective software and take other security

precautions.

"We are committed to in every way possible to tracking those who are responsible," Attorney General Janet Reno said in Washington.

Sensitive government systems were being quickly secured against potential attacks, Commerce Secretary William Daley said in a teleconference Wednesday.

"Right now there is no surefire defense, but we are trying to take some steps," he said. "First we are taking special action to ensure that all federal systems, including civilian agency systems, and those of the Defense Department, are clean of these infec-

tions, which make some systems the unwitting partner in these attacks."

Some security experts said the publicity could encourage pranksters.

"It's what these guys go after—to be known as the person or group of people who've pulled these attacks off," said Simon Perry, security business manager at Computer Associates International, a maker of business software. "Instead of graffiti on the subway wall, they've climbed up to the 40th floor of the Empire State Building and put their messages there."

The growing anxiety about the Internet's  
See HACKERS, Page A-9

*Fairbanks Daily News Miner, Feb 10, 2000, page 1A*

Fairbanks Daily News-Miner, Thursday, February 10, 2000

## HACKERS BO

Continued from Page A-1

vulnerability contributed to a 258-point slide in the Dow Jones average Wednesday and halted three straight record-high closings for the Nasdaq Composite Index, which is heavy with high-tech stocks.

The hacker technique—called a "denial of service attack"—involves directing a flood of messages to computers that run Web sites. The effect is comparable to unleashing a wave of calls to tie up a city's phone lines.

The ETrade online brokerage's Web site was hit Wednesday, but "customer accounts were never compromised," spokesman Patrick Di Chiro said. Less than one-fifth of its customers were affected by the clogged traffic for about 90 minutes before the company blunted the attack, he said.

ZDNet.com, a popular news site that covers technology, said its Web site was shut down for two hours and "appeared to have been the target of a denial-of-service attack."

Major sites attacked this week include eBay, Amazon.com, CNN, Buy.com and Yahoo!

# Web hackers widen attacks

Message flood cripples more major sites; Wall Street jittery

By DAVID E. KALISH  
The Associated Press

NEW YORK — Hackers stepped up a three-day electronic assault Wednesday against some of the most popular sites on the Web, inconveniencing millions of Internet users and unnerving Wall Street.

The apparently coordinated attacks spread to ETrade, ZDNet and other major sites Wednesday. All of them were crippled by a barrage of messages generated by hackers.

The growing anxiety about the Internet's vulnerability

---

*'Right now there is no surefire defense, but we are trying to take some steps.'*

— Commerce Secretary William Daley

---

contributed to a 258.44 point slide in the Dow Jones average and halted three straight record-high closings for the NASDAQ Composite Index, which is heavy with high-tech stocks.

The attacks also prompted top federal officials to reassure Americans that authorities are doing everything

they can to fight the on-line vandalism.

"We are committed in every way possible to tracking those who are responsible," Attorney General Janet Reno said in Washington.

She said the motives of the vandals are not known, "but

See Back Page. HACKERS

ADN, Sep 10, 2000, page A1

## HACKERS: Businesses urged to protect themselves

they appear to be intended to interfere with and disrupt legitimate electronic commerce."

The hacker technique, called a "denial of service attack," involves directing a flood of messages to computers that run web sites. The effect is comparable to erecting human barricades to block shoppers from entering a mall or unleashing a wave of calls to tie up a city's phone lines.

Hackers could face maxi-

mum penalties of 5 to 10 years behind bars and fines up to \$250,000, or in some cases "twice the gross loss to the victim," said FBI cyber-security expert Ronald Dick.

In the latest attacks, the ETrade brokerage's web site was hit, but "customer accounts were never compromised," spokesman Patrick Di Chiro said. Less than one-fifth of its customers were affected by the clogged traffic for about 90 minutes.

ZDNet.Com, which covers technology, said its site was shut down for two hours.

Microsoft's MSN.com said it was indirectly affected because of disruptions to several Internet service providers carrying its traffic. Major sites that came under attack Tuesday included eBay, Amazon, CNN and Buy.Com, all in aggressive assaults similar to one that overwhelmed Yahoo! a day earlier.

Federal officials urged

businesses to install protective software.

"Right now there is no surefire defense, but we are trying to take some steps," Commerce Secretary William Daley said. "First we are taking special action to ensure that all federal systems, including civilian agency systems, and those of the Defense Department, are clean of these infections, which make some systems the unwitting partner in these attacks."

*Journal Empire, Feb 15, 2000*

## Clinton meets computer experts

■ *Web security sought after hacker attacks; FBI has suspects*

By **SONYA ROSS**

THE ASSOCIATED PRESS

**WASHINGTON** - With the FBI seeking to question several hackers about last week's Internet attacks, President Clinton today began exploring ways to tighten security on the World Wide Web but cautioned the attacks were not an "electronic Pearl Harbor."

Surrounded by technology experts and a hacker known as Mudge, Clinton said the attacks nevertheless served as a needed wake-up call. The assault was hardly so devastating that it could be compared to Japan's bombing

of Pearl Harbor, which wiped out the Pacific Fleet and drew the United States into World War II, he said.

"It's a source of concern, but I don't think we should leave here with this vast sense of insecurity," Clinton said. "We ought to leave here with a sense of confidence that this is a challenge that was entirely predictable. It's part of the price of the success of the Internet."

Clinton gathered in the White House Cabinet Room with about 20 industry representatives, national security experts and Attorney General Janet Reno. He said the goal of the meeting was to ensure that the Internet remains "open and free."

One participant, Whitfield Diffie of Sun Microsystems, set up

his laptop on the conference table, an agenda on the screen. Mudge, in a business suit with his long brown hair hanging down on his chest, sat quietly with his fingers interlocked atop his blue briefing books.

Meantime, a computer believed to have been used in last week's attacks, was seized by federal agents, Hillsboro, Ore., Police Sgt. Allen Zaugg, head of a group of officers trained for high-tech cases, said today.

The FBI is now analyzing that computer, which was seized within the last two days from a home business in the Portland, Ore., area, a federal official in Washington said, requesting anonymity. Its owner apparently was not aware the computer was used as a middleman in the attacks, this of-

ficial said.

The threat of an "electronic Pearl Harbor" was raised in March 1999 by then-Deputy Defense Secretary John Hamre, who predicted in congressional testimony that cyberterrorists would target America's commercial interests.

The initial idea of the session was to address the problem of terrorists using cyberspace. But Clinton told CNN.com on Monday that last week's attacks underscore a need for the government to focus on protecting the Internet itself.

The FBI was seeking to interview several hackers known by their Internet screen names, including one who calls himself "mfiaboy" and another who calls himself "coolio," a Justice Department official said.

# Internet attacks raise concerns about risks of growth

By ANICK JESDANUN  
AP Internet Writer

NEW YORK — A swarm of recent hacking attacks highlight one emerging concern about the Internet: It may be growing too fast for security to keep up with technology.

Some security experts believe it's time to focus on making the Net safer, which could mean rebuilding much of the underlying infrastructure from scratch. After all, consumers and businesses now use the Internet for tasks unforeseen 30 years ago.

Security was an afterthought when Internet standards were developed by university thinkers and computer administrators, says Russ Cooper, who runs the NTBugtraq Web site devoted to security.

"This is now the foundation for billions of dollars worth of commerce," Cooper said. "It is inherently flawed because we don't check to see if what it's being used for is what it is intended for."

Randy Sandone of Argus Systems Group Inc. is blunter: "The Web is rotten at its core."

Yahoo!, Buy.com, eBay, ETrade and other prominent sites were paralyzed for hours at a time last week when hackers overloaded them with fake traffic.

The attacks followed several computer virus outbreaks last year — such as Melissa — which spread rapidly by taking advantage of functions that were designed to make Internet use friendlier.

And last month, a hacker stole credit card numbers from the Internet music retailer CD Universe, then released thousands of them on a Web site after the firm refused to pay \$100,000 ransom.

"I fully expect the Internet to ultimately be safe and stable," said Stephen Gorrell, program manager for Norton Internet Security software. "However, in the period of record growth, it's not surprising new holes are discovered."

The Internet's developers could not have effectively countered threats to commerce because e-businesses did not yet exist, Gorrell said.

As the Internet grows, so do the numbers of hackers and potential victims. And hackers are becoming more sophisticated, with some even developing tools to

---

**'I fully expect the Internet to ultimately be safe and stable. However, in the period of record growth, it's not surprising new holes are discovered.'**

---

—Stephen Gorrell, program manager  
for Norton Internet Security software

automate their attacks.

Software companies, some critics say, contribute to the problems by releasing products that still have security holes.

"Each day, technology is changing," said Robert Ing, who handles electronic security for SBR International Inc. in Toronto. "There's a rush to get products out to market because it is a competitive marketplace. Sometimes, security is overlooked."

Steve Hunt, security analyst at Giga Information Group in Chicago, hopes the latest attacks will encourage companies to take security more seriously.

"We owe quite a debt of gratitude to hackers to show us where our pants have

been down," he said.

Security and Internet experts differ on how far they need to go — and that itself is a problem. Some believe in completely updating equipment and software to reduce users' anonymity and improve authentication.

In the offline world, businesses have experience with security guards and special locks. Some practices are even required by law or insurance companies.

But the Internet community has yet to agree on such standards, said Harris Miller, president of the Information Technology Association of America.

Phil Attfield, director of technical marketing at McAfee.com, said Internet secu-

rity will eventually catch up.

"The approaches are going to have to become more formal rather than ad hoc," he said. "We've been getting there incrementally. That's the way technology is evolving."

But hacking will never completely disappear, said Keith Teare, the chairman and chief executive of RealNames. Vandals broke into RealNames' computers Wednesday, and the company had to warn some 20,000 customers that their credit card numbers might have been stolen.

"For every secure environment, there will be somebody prepared to try to break in," Teare said. "If they are clever enough, they will find holes."

Greg Hawkins, chief executive of Buy.com, said the attacks on his shopping site and others raised awareness.

"This is a new frontier. It's big, it's fast, and it's growing rapidly," he said. "With that growth will come continued challenges to make sure it's a secure and effective environment. We are clearly going to have growing pains like this from time to time."

## Catching hackers won't be easy

### FBI seeks expansion of racketeering laws against organized electronic assault

By TED BRIDIS  
AP Technology Writer

WASHINGTON — The nation's top law enforcement officials acknowledged on Wednesday serious challenges finding the electronic vandals who shut down major Internet sites last week, but they also described "fast-developing leads."

They said the hackers involved were sophisticated enough to falsify their digital fingerprints. Attorney General Janet Reno said such a disguise technique "makes it difficult, and sometimes impossible, to hold the perpetrator criminally accountable."

"I would simply say that we are taking the attacks very seriously and that we will simply do everything in our power to identify those responsible and bring them to justice," Reno told a Senate panel.

FBI Director Louis J. Freeh, who also testified, said there were "fast-developing leads as we speak, and hopefully we can provide more details in coming days." He said FBI field offices in five cities have opened investigations into the attacks: Los Angeles, San Francisco, Atlanta, Boston and Seattle. More agents in other cities and overseas are also involved.

Reno and Freeh also conceded impor-

tant shortcomings coordinating the myriad government agencies and public and private experts who help investigate high-tech crimes. "We're not doing so good," admitted Freeh, adding that cooperation was improving.

The FBI also urged Congress on Wednesday to consider expanding use of federal racketeering "RICO" laws — traditionally used against the mafia and drug cartels — to apply against organized and persistent hackers. It also urged Congress to lower the \$5,000 minimum in damages that victim companies must suffer before attackers can be prosecuted under federal computer crime laws.

Freeh said lawmakers should consider "whether some of this activity, which goes beyond a single episode of fraud or hacking, gets into the realm of enterprise criminal activity."

"RICO was intended to get gangsters," said Jennifer Granick, a California lawyer who has represented hackers. "Now, it's getting a bunch of kids in black concert T-shirts."

Freeh said hackers in many of last week's attacks falsified the Internet addresses of the computers they used, "meaning that the address that appeared on the target's log was not the true address

of the system that sent the messages."

eBay Inc. disclosed new details Wednesday about the electronic assault launched against it Feb. 8, which shut down the world's largest online auction site for 90 minutes. Similar attacks disrupted other major commercial sites, including those of Yahoo!, Amazon, Buy.Com, CNN and ETrade.

eBay's lawyer, Robert Chesnut, described an "insidious, organized attack" that was "obviously well planned."

The attackers flooded eBay's site with 10 times its normal incoming data, transmitting a specific type of information identical to that used against Yahoo! on Feb. 7.

Chesnut told the Appropriations subcommittee on Commerce, Justice, State and judiciary that eBay also was attacked the evening of Feb. 9, but engineers were able to repel the second attack quickly.

The FBI is contacting several hackers, known by their online nicknames. The bureau would not say whether its agents have talked with any suspects, but it appeared some interviews have begun, hacker sources said.

The testimony from Reno and Freeh followed President Clinton's meeting

Tuesday with technology experts about ways to improve Internet security. Participants said that during the talks, industry leaders urged the government to lead by example by making its computer systems secure.

But overnight Tuesday, a hacker vandalized at least four Web sites at the Transportation Department, including the page for the agency's information officer, George Molaski.

Those attacks were first noted by Attrition.Org, a computer security Web site that records such hacks.

The computer breached by the hacker "was in the process of being fixed," Molaski said Wednesday. "Unfortunately, they got to it before we closed that door. It was a relatively simple vulnerability."

Also Wednesday, House Commerce Chairman Tom Bliley, R-Va., criticized "highly vulnerable" computers at the Environmental Protection Agency and urging it to shut down its Internet connection immediately, citing an unreleased report by the General Accounting Office.

EPA spokesman David Cohen said the agency has no plans to disable Internet access, adding that experts there have taken steps to strengthen security of computers with sensitive information.

# Expert sees rising cyber-terror risk

By Nancy Pounds  
Journal Assistant Editor



America's growing dependence on the Internet and major industry networks has put the nation at the highest risk yet for cyber-terrorism attacks, according to one technology expert.

The nation's Internet systems are more vulnerable than other countries' operations since more than half of the Internet is in the United States, he said.

Although more cyber-crime has been identified than terrorism, the criminals could be practicing now, said Seymour Goodman, a professor at Stanford and Georgia Tech universities. He also is director of the Consortium for Research on Information Security and Policy at Stanford.

Goodman, who has visited 80 countries to offer international public policy advice on technology, spoke Feb. 25 at the Alaska World Affairs Council luncheon at the Hilton Anchorage Hotel.

Cyberspace crimes can range from robbery to intimidation to warfare, including attacking military networks, he said.

"And the United States is a prime target since we rely on these systems," Goodman said.

Alaska's vulnerability to cyberspace attacks could climb depending on the security of systems controlling a proposed National Missile Defense System that could be built in Alaska, he said.

From his experience, Goodman has seen that many network technology systems lack needed security to fend off criminals.

"We've made ourselves more vulnerable at the same time as we're taking advantage of the efficiencies of the systems," he said.

In the last 10 years, activity in cyberspace has experienced an explosion, especially in Internet users and networks that power industries like the banking and finance sector, Goodman said.

Started 30 years ago, the Internet has grown from the six countries connected 15 years ago to 214 entities today, he said. Each year the Internet grows another 50 percent to 100 percent.

"This represents one of the most rapid infusions of technology," Goodman said.

Accompanying growth is increased efficiency and connectivity, which in turn spurs greater dependence on Internet

## TECHNOLOGY

and network systems, he said.

"I would argue that what has happened in cyberspace, particularly in the last 10 years, is that we have created a new medium of great importance for a tremendous spectrum of human activity," Goodman said.

This technology-driven medium, similar to physical media of air, sea and land, is the stage for social and financial transactions on a large scale, he said.

However, the systems that make up the Internet often lack security as a main function, according to Goodman.

One of Goodman's Stanford colleagues was one of the initial Department of Defense Internet operators who says that as early Internet programmers, they did not design security into the operation, but planned to come back to it. But now the Internet is much more complex, Goodman said.

Vulnerable systems lead to more opportunities for conflict, whether it's offensive content or decaying ethics, he said. Also, from the standpoint of crime, there are increased opportunities for terrorism because terrorists can be distant from their victims, he said. "Crime out there on the Internet is growing as quickly as the Internet itself.

"Some of us think that we still need to civilize cyberspace.

Otherwise it will be like the wild West. But how do we do that? This is an international, borderless medium."

One means of defense is passive — making computers less easy to hack, he said. But without a penalty for breaking in, attackers will try until they succeed or become bored, he added.

An active defense includes collecting evidence in the difficult task of apprehending cyberspace criminals internationally, although this plan requires countries to agree on what would be considered a crime, he said.

The cost of technology crime won't be paid by industries or governments, Goodman said.

"We as individuals will pay for this if it's not fixed, or we will pay as a nation if a terrorist attack occurs," he said.



## Selling Your Company?

Let Me Help.

- Consultation
- Value Assessment
- Packaging
- Results

**Matthew Fink**

Commercial Properties/Business Specialist

3111 'C' Street, Suite 100 • Anchorage, Alaska 99503

Office (907) 261-7620 • Fax (907) 261-7685

**DYNAMIC  
PROPERTIES**

## LATESPORTS



John Smoltz: Injury ends season.



Boomer Esiason: Sacked by ABC.



Dennis Rodman: Released by Mavs.

## They're out

IC

# USA TODAY

NO. 1 IN THE USA... FIRST IN DAILY READERS

## GOD LI TOAST PASTR

God, the Dev  
is a new TV  
whimsical tw  
Almighty loo  
Garcia, an au  
must save the  
Satan has an  
accent. A rev

THURSDAY MARCH 9, 2000

## NEWSLINE

A QUICK READ ON THE NEWS

**WALL STREET:** Dow Jones industrial average jumps 60.50 points to 9856.53; Nasdaq Index soars 49.33 points to 4897.17; 30-year Treasury bond yield climbs to 6.16%. 1,4B.  
 ▶ **USA TODAY Internet 100** rises 0.88 points to 189.04. 4B.  
 ▶ **Japan's Nikkei** average is up 119 points to 19,886 midday; yen is 107.04 per dollar. Hong Kong's Hang Seng Index is 198 points to 18,149 early today.

### Four killed in Memphis ambush



By A.J. Wolfe, The Commercial Appeal, via AP

**Aftermath:** Firefighters console one another Wednesday after arriving at a house fire and being shot at by an off-duty firefighter; four people were killed and two were injured. 4A.

**OIL PRICES FALL:** OPEC pledge to provide "adequate and timely oil supplies in coming months" is linked to a more than 8% drop in crude oil prices. 1B.

**SOUTHWEST AIRLINES CRASH:** Pilots are blamed for approaching Sunday's landing in California too fast and too steep. 3A.

**FASTEST-GROWING COUNTY:** Virginia's Sussex County zooms from 10,000 to more than 12,000 from 1998-99, thanks to two new prisons and 2,400 inmates. 3A.

**TODAY'S DEBATE:** Interest rate hikes. In USA TODAY's opinion, "Greenspan hits the brakes. Risky? Yes. But less risky than letting inflation take hold."  
 ▶ "We are in a New Era economy that is different from the economics of the past. As a result, it requires a different monetary policy," Brian S. Wesbury says.

**MONEY:** Homebuyers basking in new no-down payment, 100%-plus mortgages; experts express concern. 1B.  
 ▶ Low-cost Linux is giving Windows a run for its money. 1B.  
 ▶ Traffic safety officials warn about use of vans instead of buses to transport students. 1B.  
 ▶ Miller rolling out beer in plastic bottles. 3B.

**SPORTS:** Tony Hawk has turned skateboarding into big bucks. Critics wonder whether that's a good deal. 3C.  
 ▶ Buffalo tops Boston in overtime 2-1. NHL. 13-14C.

**LIFE:** Marketing firms that work for drug companies teach doctors about the products, raising ethical flags. 1D.  
 ▶ Andrew Huebner writes a haunting first novel about the Indian wars. Books, reviews, best sellers. 6-8D.

**CORRECTION:** Rhode Island election results were transposed in some editions Wednesday. McCain won the state over Bush 60%-36%. Super Tuesday results. 14A.

Written by John O. Buckley



By Tom Iker for USA TODAY

Watched her system get bused: Susan Levy Haskell of the University of Minnesota.

# How the government failed to stop the world's worst Internet attack

By M.J. Zuckerman  
USA TODAY

Susan Levy Haskell arrived at her office at the University of Minnesota as usual before 8 a.m. on Monday, Aug. 16, 1999, where she watched at first curiously, then later in horror, as the university computer system came under attack from a massive yet anonymous Internet adversary.

Haskell, the university's computer security coordinator, says that as hours passed the volume of incoming malicious traffic rose from a mere annoyance to an all-consuming, electronic dissonance. The Internet connection grew ever less responsive, degrading steadily until the university was cut off from the world.

"It became pretty terrifying to realize how many machines had to be involved. It seemed like hundreds."

Investigators later determined that 2,200 computer systems, including those at more than 30 universities in the United States, had become unwitting "zombies," serving a still unidentified master computer, which directed the attacks and forced the university off the Internet for two days.

In a matter of weeks after the Minnesota incident, academics and elite computer security firms began

spreading the word to clients and colleagues that this newly enhanced "denial of service" (DoS) attack was a clear and immediate danger to the Internet.

But it would take more than a month before federal officials at the National Infrastructure Protection Center (NIPC), which is responsible for national computer security matters, to learn of the incident and three more months for them to conclude that it was a threat worthy of a warning to the public.

It is now apparent that throughout the end of 1999, cybervandals were infecting large, insufficiently secured computer systems as zombies and laying the groundwork for a series of attacks last month that rocked e-commerce.

The delayed response and limited distribution of threat information is one of several criticisms being leveled at the NIPC and its sister agencies as the investigation into the attacks progresses slowly, according to recent congressional testimony.

"It was not enough," says Jamie Gorelick, the former deputy attorney general, who from 1994 to 1997 directed the administration's creation of the current electronic defense policy.

### COVER STORY

Please see COVER STORY next page ▶

**COVER STORY****Agencies defend their response**

Continued from 1A

She and others say the protection center failed, leaving many e-commerce firms unprepared for the attacks Feb. 8-11 that slowed the global Internet by 20% and shut down the world's most popular commercial Web sites and the FBI's home page.

"There needs to be some agile operational capacity in the government, an ability to move quickly to provide warnings," she says. "This doesn't sound at all like what we had in mind."

Michael Vatis, director of the NIPC, an interagency fusion of federal, local and international organizations based at the FBI, defends his agency's response. It says it permitted the private sector to prepare for the worst while avoiding public hysteria.

"Three years ago we wouldn't have been able to respond at all," Vatis says. "Today we have an effective resource" for investigating crimes and issuing threat alerts.

Critics say the protection center and its sister agencies have fallen short of the vision President Clinton had two years ago when he issued a plan to "create a genuine public-private partnership to protect America in the 21st century" from devastating cyberattacks. The plan called for the private sector, which owns and operates both the Internet and the infrastructure that supports it — electricity, banking and communications — to create secure information-sharing centers in which companies could anonymously share threat information, new vulnerabilities and crises data. It also created a Commerce Department coordinating center to work with those industry clearinghouses and the NIPC.

But as the administration seeks \$37 million in new spending for cybersecurity, the NIPC and its sister agencies are troubled by confusion within their own ranks as well as a lack of cooperation from companies and other government agencies:

► Other government agencies are refusing to work with the NIPC, privately pointing to the FBI's longstanding reputation for not sharing well with others. "That's something we're still working on," Vatis says.

The Pentagon is the only Cabinet-level agency represented at the NIPC. The Secret Service, Transportation Department and Treasury Department, each of which is designated to have

**"There needs to be some agile operational capacity in the government, an ability to move quickly to provide warnings. This (last incident) doesn't sound at all like what we had in mind."**

— Jamie Gorelick, former deputy attorney general

representation at the protection center, refuse to take part. The Department of Energy, which is supposed to play a major role at the center, is not represented. The CIA, which has four slots at the center, has filled one.

► Friction and turf battles between the new cybersecurity agencies may be hampering operations. The National Coordinator for infrastructure protection and counterterrorism is Richard Clarke, a White House official, who must get clearance on a case-by-case basis before the NIPC will brief him about investigations.

Vatis says Justice Department guidelines bar the FBI from briefing anyone outside the department about ongoing cases unless the attorney general grants a waiver.

► The Internet communi-

ty is demanding broader distribution of more timely threat in-

formation. "We're treating their computers as attack 'zombies.'" On Dec. 8, the NIPC sent a note briefing FBI Director Louis Freeh for the first time. On Dec. 17, Vatis personally briefed Attorney General Janet Reno as part of an overview of preparations being made for Y2K.

By that point, several DoS attacks already had occurred, but "people weren't getting the message," Dittrich says. "CERT and NIPC were really worried. They had obviously been hearing about a lot more intrusions. They went back and recategorized a whole bunch of incident reports going back to April-May time frame, and they started telling me that this is a really big thing."

But not until the NIPC, working with Dittrich and Mitre Corp., developed a tool for identifying zombies in a system did the protection center decide to warn the public Dec. 30 and post the tool for anyone to download.

By that time, Vatis says, "someone was setting the groundwork for an attack, and that is when we decided to make a public announcement."

**Electronic 'night of the living dead'**

The NIPC was convinced that New Year's Eve "could be a day for people to start sending marching orders to these zombies. We were afraid that Dec. 31 might become the night of the living dead," he says.

"Thanks for giving us plenty of time to prepare," says a sarcastic Vinton Cerf, an MCI WorldCom executive who is widely regarded as a founder of the Internet. "The timing of this all was singularly unfortunate."

But the protection center gets high praise from many security firms for being the first to provide an effective tool to locate and remove the zombie infections. Vatis says far more damage would have occurred in February otherwise.

"You know, I'm sensing a little bit of doublespeak here," Vatis says. "Business is saying, 'We don't want the government telling us what to do; we can fix this ourselves.' And I agree. But then I hear people saying, 'Gosh, government didn't warn us loud enough.'"

"People have been saying for a long time that it's going to take an electronic Pearl Harbor for people to take security seriously," he says. "There's a kernel of truth there because we live in an event-driven society."



► The Internet community is demanding broader distribution of more timely threat information, beyond the security professionals with whom the NIPC typically deals. "If you are only spreading the word to specialists, then you are not getting threat information out across the board to small universities or e-tailers," says Harris Miller of the Information Technology Association of America, a leading trade association representing 11,000 corporations.

► Though some companies are warming to the idea of sharing information with the government, many complain that they remain uneasy about government efforts to police the Internet.

"Where (the federal government) is completely failing is to be a place people trust" with delicate information, says Alan Pallar of the SANS Institute, an education facility for computer system administrators that claims 100,000 members. "Ninety-eight percent of the time they won't share with the FBI because they fear having their (computers) confiscated, that their troubles will become public knowledge and that the agents will scare (clients) to death."

► The president's plan has created so many entities gathering data on Internet vulnerabilities that it is causing confusion. "Imagine living in a community where there are seven different numbers to call for 911 services," says Mark Rasch, chief counsel to Global Integrity, a leading cybersecurity firm that hosts the financial industry's information sharing center. "You need to have one number, one place, that everyone trusts."

Adds Tom Noonan, CEO of Internet Security Systems, probably the fastest-growing firm in its field and a major booster of the NIPC: "Quite frankly, I'm confused by all these different government groups."

### Word spreads slowly

In the days after the University of Minnesota attack, Haskell says her 911 instinct was to notify academic colleagues or other trusted computer professionals.

One of those she contacted was David Dittrich, director of software engineering at the University of Washington in Seattle. He became the first person to track down and unlock the codes that make the attacks operate.

It was a matter of days before he realized the new attack technique required immediate action. But the wheels of government turn slowly.

Dittrich first alerted CERT, the Computer Emergency Response Team at Carnegie-Mellon University, the nation's premier clearinghouse for data on computer vulnerability. By early September, it began organizing an unprecedented international conference to examine the emerging threat.

Based on CERT's letters of invitation to the conference, a handful of high-end security firms learned of the attack technique, and in October and November the firms quietly briefed clients about the impending threat.

Though the NIPC is a sponsor of CERT and has a liaison for the emergency response team on its staff, it received its first substantial report from CERT in late October. The response team has declined to comment on the apparent delay.

The three-day CERT conference in early November adjourned with this determination: "There is essentially nothing a site can do with currently available technology to prevent becoming a victim" of a denial-of-service attack.

The only prevention, the conferees said, was for system operators to update their security precautions to prevent vandals from exploiting known system weaknesses to gain control of



**Office space a**  
Prime location, h  
Internet access,  
generous vacatio

Take your office on the road with high



Closing the deal on the way to breakfast



Editorial and publication headquarters:  
1000 Wilson Blvd., Arlington, VA 22229  
Phone: 703-276-3400

Published by Gannett Co., Inc. Volume 18, No. 125 (ISSN 0734-7456)

Subscriptions and general information:  
1-800-USA-0001

Hours: Mon. - Fri. 6:30 a.m. - 9 p.m. Eastern Time.  
Subscription rates in the U.S.: 13 wks. \$39; 26 wks. \$78; 39 wks. \$117; 52 wks. \$156. Rates to foreign countries available. Send correspondence about subscriptions to Sheila Kogge, Director of National Customer Service, P.O. Box 4179, Silver Spring, Md. 20914. Fax subscription information: 1-800-732-3631  
Deaf or hard of hearing with TTY equipment: 1-800-331-1706

Classified advertising: 1-800-USA-CLAS  
All advertising published in USA TODAY is subject to the current applicable rate card, copies of which are available from the advertising department. USA TODAY may, in its sole discretion, edit, classify, reject or cancel at any time any advertising submitted by an advertiser.  
National and Regional advertising: 1-800-242-5858  
Reprint permissions, copies of articles, glossy reprints: 703-558-5619 Fax: 703-247-3133

Seattle Times 12 Nov 2000

# Hackers' Web-site assaults take toll

*Victims and experts call randomness frightening*

BY PETER LEWIS  
*Seattle Times technology reporter*

Compared with a street mugging, an attack on a Web site lacks a certain reality. The "crime" seems thin, the consequences soft.

Tell that to Blaine Hadlock, owner of a small, Bainbridge Island-based business that got hacked last year, allegedly by a total stranger who turned out to be a computer-science student in Boston. When Hadlock finished



JIMI LOTT / THE SEATTLE TIMES

**Blaine Hadlock**, owner of Zebra Marketing Online Services, changed his business plan after a hacker attack.

picking up the pieces, the tab exceeded \$30,000.

It is a phenomenon expected to grow worse before it improves, said Richard Power, spokesman for the Computer Security Institute, a San Francisco-based association of information security professionals.

"As the cybercrime problem grows, the smaller and medium-sized businesses will be more

targeted for fraud or malicious mischief," predicted Power, "simply because there will be more sharks in the water interested in smaller prey."

What's particularly disturbing is the apparent randomness of such attacks. Hackers can use fairly simple scanning programs to hunt for vulnerable systems.

PLEASE SEE *Hack*

D 2  
he  
re

# After attack, victim takes his company out of harm's way

## HACKERS

CONTINUED FROM D 1

"It did not put us out of business, but it stung real bad," recounted Hadlock, whose Zebra Marketing Online Services (ZMOS) has five full-time employees and has since moved to Federal Way. "You don't lose that kind of money without it hurting you. It caused me some significant problems."

Authorities contend the hacker is a Northeastern University student named Ikenna Ifih, who in federal charges filed recently in Boston was also accused of illegally entering federal computers at the National Aeronautics and Space Administration and the Defense Department.

Last spring, investigators with the FBI and the Department of Defense kept asking Hadlock, "Why you? Why him?"

And Hadlock had a stock answer: "Ask him (the hacker)."

"I really don't know from whence he came and why. I'd love to sit with him and ask 'Why?'"

Power, with the security institute, said the public often has difficulty understanding the motive behind such stranger-on-stranger cyber attacks. "People say, 'Well, why do they do this?' And the answer they can't understand is, 'Just because,'" Power said.

He said attacks on smaller businesses are particularly damaging because the owners cannot absorb the hit like a major corporation, and they generally lack insurance to cover such losses.

Assistant U.S. Attorney Steve Schroeder of Seattle, who helped investigate the ZMOS case, agrees.

"It's the smaller systems that can't afford to spend resources on security that are going to remain vulnerable," he said. "The little mom-and-pop sites. If a hacker attack would bury them."

Most of the hacking incidents Schroeder is aware of in Western Washington involve stranger-on-stranger attacks. Several remain under active investigation. But another threat comes from disgruntled employees.

That's what occurred to small-business owner Bud Robinson, who runs an ice-machine rental business called Automatic Ice Makers in San Diego. Two years ago, a disgruntled programmer "just walked out one day and said 'I'm going to own you,'" Robinson recalled.

Before leaving, the employee placed some malicious code in the system — a "logic bomb" that

disabled access and caused about \$50,000 in damage. It took nearly two years for Robinson to recover, repairing the system in stages as he could afford to.

James Crowell, aka Jamie Crowell, ultimately pleaded guilty to a felony charge of recklessly damaging a protected computer. Crowell was sentenced to serve six months in a halfway house and ordered to make restitution, among other conditions.

In Hadlock's case, the intrusion influenced him to shift business models. Instead of hosting other companies' Web pages, ZMOS now acts as an "e-business facilitator," Hadlock said, meaning the company helps e-businesses figure out what their message is and provides marketing assistance.

Besides being disruptive, Hadlock said the attack caused him to realize how legally vulnerable he was as the guardian of other people's information. If a Web-hosting company is housing "hundreds or thousands or millions of dollars' worth of (intellectual-property) investment and somebody (a hacker) gets to you, guess who is on the line?" Hadlock asked rhetorically.

"So we changed after this little scenario," he said. "It led us to not being in that (Web-hosting) business."

As far as prosecutors know, ZMOS was the most seriously damaged victim. Ifih's other alleged unauthorized forays caused no disruption to the nation's defenses, no meddling with satellite control, and no improper use of personal information — including private information on about 9,000 students, faculty and alumni at Northeastern that Ifih is accused of downloading and copying.

The 28-year-old student now faces three felony counts related to unauthorized access to various computers. If convicted, he could serve up to 15 years in prison and pay a \$250,000 fine.

Ifih was charged by criminal information instead of indictment, which generally is a sign that a plea agreement is in the works.

Authorities have asserted that Ifih also went by the hacker name "DigiAlmty" and that he was responsible for defacing an Interior Department Web page. On that page, Ifih is accused of writing in part: "Yes, you guessed it right, the WAR is on. The (expletive) FBI vs. everyone who calls him-herself a true hacker."

Peter Lewis: 206-461-2217. E-mail: [plewis@scattletimes.com](mailto:plewis@scattletimes.com)

*"People say, 'Well, why do they do this?' And the answer they can't understand is, 'Just because.'"*

RICHARD POWER

Spokesman, Computer Security Institute

anon Daily News 12 mar 2000

# Cookies' maker chews over their fate

By THOMAS E. WEBER  
The Wall Street Journal

Cookies, those tiny computer files that web sites use to track visitors, have come to symbolize the worst fears about on-line privacy. But the man who baked up the very first batch says that's just not fair.

"They're actually relatively harmless," said Lou Montulli, the computer whiz who invented cookies in 1994 and went on to be named "Sexiest Internet Mogul" by People magazine last year.

Montulli's brainchild has evolved into one of the Web's most pervasive technologies, invisibly shoring up everything from e-commerce to on line advertising. If you spend much time on the Web, chances are you've accumulated anywhere from dozens to hundreds of cookies on your PC.

Lately Internet companies have figured out how to make them do all sorts of tricks their creator didn't foresee. On-line ad network DoubleClick has turned them into huge consumer dossiers, and now finds itself under scrutiny from consumers and the Federal Trade Commission for its efforts.

The tale of how and why the cookie came to be — and why it now arouses such fears among Internet users — is a dramatic example of how the on-line world has been shaped by the decisions of a few key people. It also shows how those decisions can morph in unintended ways as the Net evolves at breakneck speed.

In the summer of 1994, Montulli was a young college dropout at a brand-new company called Netscape. It wanted to commercialize the Internet, which meant making it possible for people to buy things on-line. The problem was, web sites made poor shopkeepers. Designed to treat all requests for information separately, sites couldn't perceive individual shoppers at the other end of the line. All they saw were flurries of

unrelated queries.

That meant you couldn't mark items as you browsed for later purchase. Instead of paying for everything at once, consumers would have been forced to buy their CDs and books one at a time. The challenge for Montulli was to get a web site to see its users as distinct individuals so that it could remember things about them.

His answer was the cookie, a tiny computer file that could be stored on a user's PC. (Programmers had long used the term to refer to an arbitrary piece of data.) With a cookie, a web server essentially says: Here, hang on to this file and show it to me the next time you ask me something. It will remind me who you are and what we've already talked about.

Netscape built cookies into the first version of its browser, making them a de facto standard for the Web. Like any good programmer, Montulli designed cookies to be flexible. "Netscape was about building the infrastructure for the Web," he said. "We tried to build things that would be useful for the entire community."

Use it they did. When web sites began to run paid advertisements, advertisers wanted to know the size of the audience. Sites counted up "hits," but couldn't tell if 10 hits represented 10 different users or one person visiting 10 times. By assigning each visitor a unique cookie, sites could discern one visitor from another and make accurate tallies.

From there, it wasn't much of a leap to use cookies to track visitors' habits, noting things like which pages they visited most frequently. DoubleClick, which sells advertising on a network of sites, figured it could charge more for ads if they were targeted based on consumer behavior.

Now DoubleClick wants to go a step further, matching up cookie data with information in traditional direct-mar-

keting data bases. Faced with a company that can potentially track where you surf and knows your mail-order shopping habits to boot, some consumers have started getting anxious. Earlier this month, DoubleClick disclosed that the FTC was examining its practices, which depend heavily on cookies.

Montulli, 29 years old, says DoubleClick and dozens of other web marketers are using cookies in ways he never intended. But he admits his design gave an unintended boost to tracking efforts. Here's why: When a web site displays a page you've requested, it can pull elements, including ads, from other sites. That allowed ad networks to put their own cookies on consumers' PCs and track them across many sites. Montulli later added to Netscape an option that lets users refuse cookies from sites other than the one they're visiting.

Efforts to reform cookies further haven't met with much success. After building cookies into Netscape Navigator, Montulli helped develop an official standard for the Internet Engineering Task Force.

The proposal calls for each cookie to include a description of its purpose so consumers could inspect their cookies and find out what they're up to.

The idea hasn't gotten very far. The fact is, it's too late to tinker with cookies now. They power practically every on-line shopping cart and every paid advertisement. In less than six years, they've become part of the fabric of the Web.

A lot has changed for Montulli in that time. Once the quintessential unkempt geek, he's now a Netscape millionaire with a steady girlfriend, a great haircut and stylish clothes. The People magazine story even compared him to hunky actor Dylan McDermott.

He's working at a buzzy start-up called Epinions.com, a shopping guide where visitors can read and post product reviews. Naturally, it uses cookies.

# EXTINCTION: Exec warns of technology

Continued from Page A-1

Joy is disturbed by a suite of advances. He views as credible the prediction that by 2030, computers will be a million times more powerful than they are today. He respects the possibility that robots may exceed humans in intelligence while being able to replicate themselves.

He points to nanotechnology — the emerging science that seeks to create any desired object atom by atom — and agrees that it has the potential to allow inexpensive production of smart machines so small they could fit inside a blood vessel. Genetic technology, meanwhile, is inexorably generating the power to create new forms of life that could reproduce.

What deeply worries him is that these technologies collectively create the ability to unleash self-replicating, mutating, mechanical or biological plagues. These would be "a replication attack in the physical world" comparable to the replication attack in the virtual world that recently caused the shutdowns of major commercial web sites.

"If you can let something loose that can make more copies of itself," Joy said, "it is very difficult to recall. It is as easy as eradicating all the mosquitoes. They are everywhere and make more of themselves. If attacked, they mutate and become immune... That creates the possibility of empowering individuals for extreme evil. If we don't do anything, the risk is very high of one crazy person doing something very bad."

What further concerns him is the huge profits from any single advance that may be beneficial in itself. "It is always hard to see the bigger impact while you are

in the vortex of a change," Joy wrote. "We have long been driven by the overwhelming desire to know that is the nature of science's quest, not stopping to notice that the progress to newer and more powerful technologies can take on a life of its own."

Finally, he argues, this threat to humanity is much greater than that of nuclear weapons because those are hard to build. By contrast, he says, these new technologies are not hard to come by. Therefore, he reasons, the problem will not be "rogue states but rogue individuals."

Joy's critique is striking because computer industry technologists, almost without exception, take a more sanguine view of the social consequences of advances. They typically argue that any negative effects will be far outweighed by the positive effect of new technologies.

Nathan Myhrvold, a physicist on leave from his job as the chief technology officer at Microsoft Corp., said in an e-mail interview: "People have made apocalyptic predictions about technology constantly for as long as there has been technology. I think it is because change frightens them. What is more, the most common form these dire predictions take is 'this next generation of stuff — wow! that is really different and really scary.'"

Asked if he thinks a technological species could expect to survive the accelerating evolution of its market-driven technologies, Joy said: "The answer is yes but not without additional care. I think it's possible but it's not a given. Survival won't come for free."

□ The New York Times contributed to this story.

# Technology creator warns of its threat to mankind

ADN 13 Mar 2000

By JOEL GARREAU  
The Washington Post

A respected creator of the Information Age has written an extraordinary critique of accelerating technological change in which he suggests that new technology could cause "something like extinction" of humankind within the next two generations.

The alarming prediction, intended to be provocative, is striking because it comes not from a critic of technology

but rather from a man who invented much of it: Bill Joy, chief scientist and co-founder of Sun Microsystems Inc., the leading web technology manufacturer.

Joy was an original co-chairman of a presidential commission on the future of information technology. His warning, he said in a telephone interview, is meant to be reminiscent of Albert Einstein's famous 1939 letter to President Roosevelt alerting him to

the possibility of an atomic bomb.

In a 24-page article in the April issue of Wired magazine that hits stands today, Joy says he finds himself essentially agreeing, to his horror, with a core argument of the Unabomber, Theodore Kaczynski — that advanced technology threatens humans.

"I have always believed that making software more reliable, given its many uses, will make the world a safer and better place," Joy writes in

the article, which he worked on for months. "If I were to come to be the opposite, then I would be morally obligated to stop this work. I can imagine that such a day may come." Joy enjoys a level-headed reputation in the industry.

"Nobody is more phlegmatic than Bill," said Stewart Brand, an Internet pioneer. "He is the adult in the room."

See Back Page, EXTINCTION

# EXTINCTION: Exec warns of technology

Continued from Page A-1

Joy is disturbed by a suite of advances. He views as credible the prediction that by 2030, computers will be a million times more powerful than they are today. He respects the possibility that robots may exceed humans in intelligence while being able to replicate themselves.

He points to nanotechnology — the emerging science that seeks to create any desired object atom by atom — and agrees that it has the potential to allow inexpensive production of smart machines so small they could fit inside a blood vessel. Genetic technology, meanwhile, is inexorably generating the power to create new forms of life that could reproduce.

What deeply worries him is that these technologies collectively create the ability to unleash self-replicating, mutating, mechanical or biological plagues. These would be "a replication attack in the physical world" comparable to the replication attack in the virtual world that recently caused the shutdowns of major commercial web sites.

"If you can let something loose that can make more copies of itself," Joy said, "it is very difficult to recall. It is as easy as eradicating all the mosquitoes. They are everywhere and make more of themselves. If attacked, they mutate and become immune. ... That creates the possibility of empowering individuals for extreme evil. If we don't do anything, the risk is very high of one crazy person doing something very bad."

What further concerns him is the huge profits from any single advance that may seem beneficial in itself.

"It is always hard to see the bigger impact while you are

in the vortex of a change," Joy wrote. "We have long been driven by the overarching desire to know that is the nature of science's quest, not stopping to notice that the progress to newer and more powerful technologies can take on a life of its own."

Finally, he argues, this threat to humanity is much greater than that of nuclear weapons because those are hard to build. By contrast, he says, these new technologies are not hard to come by. Therefore, he reasons, the problem will not be "rogue states but rogue individuals."

Joy's critique is striking because computer industry technologists, almost without exception, take a more sanguine view of the social consequences of advances. They typically argue that any negative effects will be far outweighed by the positive effect of new technologies.

Nathan Myhrvold, a physicist on leave from his job as the chief technology officer at Microsoft Corp., said in an e-mail interview: "People have made apocalyptic predictions about technology constantly for as long as there has been technology. I think it is because change frightens them. What is more, the most common form these dire predictions take is 'this next generation of stuff — wow! that is really different and really scary.'"

Asked if he thinks a technological species could expect to survive the accelerating evolution of its market-driven technologies, Joy said: "The answer is yes but not without additional care. I think it's possible but it's not a given. Survival won't come for free."

□ The New York Times contributed to this story.

# Technology creator warns of its threat to mankind

By JOEL GARREAU  
The Washington Post

A respected creator of the Information Age has written an extraordinary critique of accelerating technological change in which he suggests that new technology could cause "something like extinction" of humankind within the next two generations.

The alarming prediction, intended to be provocative, is striking because it comes not from a critic of technolo-

gy but rather from a man who invented much of it: Bill Joy, chief scientist and co-founder of Sun Microsystems Inc., the leading web technology manufacturer.

Joy was an original co-chairman of a presidential commission on the future of information technology. His warning, he said in a telephone interview, is meant to be reminiscent of Albert Einstein's famous 1939 letter to President Roosevelt alerting him to

the possibility of an atomic bomb.

In a 24-page article in the April issue of Wired magazine that hits stands today, Joy says he finds himself essentially agreeing, to his horror, with a core argument of the Unabomber, Theodore Kaczynski — that advanced technology threatens humans.

"I have always believed that making software more reliable, given its many uses, will make the world a safer and better place," Joy writes in

the article, which he worked on for months. "If I were to come to be the opposite, then I would be morally obligated to stop this work. I can imagine that such a day may come when Joy enjoys a level-headed reputation in the industry."

"Nobody is more phlegmatic than Bill," said Stewart Brand, an Internet pioneer. "He is the adult in the room."

See Back Page, EXTINCTION

AD 13 Mar 2000

# Unsolicited e-mail

## Statutes

THE  
JOHN MARSHALL  
LAW SCHOOL  
CHICAGO

CENTER FOR INFORMATION TECHNOLOGY & PRIVACY LAW

Cyberspace Law: Subject Index: E-Mail

## State statutes and pending bills (United States)

- Alaska House Bill 491 (1998) **[not enacted]**  
(would have required unsolicited commercial e-mail messages to be clearly identifiable as advertisements, and to identify the sender and include opt-out instructions)
- California Assembly Bill 1629 (1998) **[enacted 9/26/98]**  
(permits ISPs to sue those who send unsolicited commercial messages in violation of an ISP's policy if the sender has actual notice of the policy, possibly including a notice embedded in the e-mail server software, and imposes criminal penalties upon those who cause computer system disruptions by using a false domain name to send messages; as the bill was originally introduced, it would have prohibited unsolicited e-mail advertisements)
- California Assembly Bill 1676 (1998) **[enacted 9/26/98]**  
(requires unsolicited e-mail advertisements to include opt-out instructions with a toll-free telephone number or a valid return address; requires senders to honor opt-out requests; and requires certain e-mail advertisements to contain "ADV:" or "ADV:ADLT" at the beginning of the subject line)
- Colorado House Bill 1284 (1997) **[enacted 4/24/97]**  
(provisions relating to e-mail were deleted prior to enactment; as introduced, the bill would have regulated but not prohibited unsolicited e-mail solicitations)
- Connecticut House Bill 6558 (1997) **[not enacted]**  
(passed by House but not voted upon by Senate; would have prohibited unsolicited e-mail advertisements)
- Illinois House Bill 2616 (1999)
- Illinois House Bill 2718 (1999)
- Kentucky House Bill 41 (1998) **[not enacted]**  
(would have required unsolicited commercial e-mail messages to identify the sender and include opt-out instructions)
- Maryland House Bill 140/Senate Bill 222 (1998) **[enacted 4/13/98]**  
(prohibits use of e-mail with intent to harass, with an exception for "peaceable activity intended to express political views or provide information to others")
- Maryland House Bill 1114 (1998) **[not enacted]**  
(would have prohibited commercial solicitations by electronic mail)
- Massachusetts House Bill 4581 (1997) **[not enacted]**  
(would have prohibited unsolicited e-mail advertisements)

- Massachusetts House Bill 4104 (1999) [status]  
(introduced in January 1999 and referred to committee; would prohibit intra-state unsolicited commercial e-mail messages)
- Nevada Senate Bill 13 (1997) [enacted 7/8/97]  
(requires unsolicited commercial e-mail messages to identify the sender and include opt-out instructions; as originally introduced, the bill would have prohibited most unsolicited e-mail advertisements)
- New Hampshire House Bill 1633 (1997) [status]  
(prefiled in December 1997; failed House vote in March 1998 following unfavorable committee report; would prohibit unsolicited e-mail advertisements to customers of ISPs that register with the state as "restricted solicitation electronic mail providers")
- New Jersey Assembly Bill 295 (1998) [status]  
(introduced in January 1998; amended by committee in June 1998 to include e-mail as well as telephone solicitations; would prohibit unsolicited e-mail advertisements)
- New Jersey Assembly Bill 513 (1998) [status]  
(introduced in January 1998 and referred to committee; would prohibit unsolicited e-mail advertisements)
- New York Senate Bill 3524/Assembly Bill 6805 (1997) [status]  
(referred to committees in March 1997; would regulate but not prohibit unsolicited e-mail advertisements)
- North Carolina House Bill 1744 (1997) [status]  
(introduced in June 1998 and referred to committee; would require unsolicited commercial e-mail messages to be clearly identifiable as advertisements, and to identify the sender and include opt-out instructions)
- Rhode Island Senate Bill 1073 (1997) [status]  
(introduced in May 1997 and referred to committee; would broaden existing law prohibiting unsolicited fax advertisements to also include e-mail)
- Texas House Bill 1773 (1999) [status]
- Virginia House Bill 1325 (1998) [status]  
(introduced in January 1998 and referred to committee, which continued the bill until 1999; would require ISPs to determine types of unsolicited e-mail messages that their subscribers do not wish to receive)
- Virginia House Bill 1668, House Bill 1714, and Senate Bill 881 (1999) [status: HB 1668, HB 1714, SB 881]  
(passed by the General Assembly in February 1999 and awaiting the Governor's signature; among other provisions, these bills make it a crime to send unsolicited bulk e-mail containing false message headers, or to sell software designed to do so)
- Washington House Bill 2752 (1998) [enacted 3/25/98] [campaign site]  
(prohibits false headers and misleading subject lines in unsolicited commercial e-mail messages, and

creates a task force to consider the need for further legislation; as originally introduced, the bill would have prohibited most unsolicited e-mail advertisements)

- [Washington House Bill 1037 \(1999\)](#)
- [Wisconsin Senate Bill 283 \(1997\) \[not enacted\]](#)  
(would have broadened existing law prohibiting unsolicited fax advertisements to also include e-mail)
- [Wisconsin Senate Bill 33 \(1999\) \[status\]](#)

---

[Subject Index](#) | [FAQ](#) | [Update service](#) | [Submit an item](#) | [Broken links](#) | [Comments](#)

1999/03/05

Homepage • News • Money • Life • Sports • Weather • Marketplace



SHOP AT  
MARKETPLACE

The Nation's e-mail news to start your day.  
**DAILY BRIEFING**  
 featuring **News** from around the globe.  
 USATODAY.com

USA  
TODAY **Nation**

**OnVia**  
All of your small business needs.

**iTool**  
Build your own e-commerce site today.

**Point.com**  
Cellular plans, phones and accessories.

02/13/00 - Updated 11:59 PM ET

## Web attacks raise concerns about growth

NEW YORK (AP) - A swarm of recent hacking attacks highlight one emerging concern about the Internet: It may be growing too fast for security to keep up with technology.

Some security experts believe it's time to focus on making the Net safer, which could mean rebuilding much of the underlying infrastructure from scratch. After all, consumers and businesses now use the Internet for tasks unforeseen 30 years ago.

Security was an afterthought when Internet standards were developed by university thinkers and computer administrators, says Russ Cooper, who runs the NTBugtraq Web site devoted to security.

"This is now the foundation for billions of dollars worth of commerce," Cooper said. "It is inherently flawed because we don't check to see if what it's being used for is what it is intended for."

Randy Sandone of Argus Systems Group Inc. is blunter: "The Web is rotten at its core."

Yahoo!, Buy.com, eBay, ETrade and other prominent sites were paralyzed for hours at a time last week when hackers overloaded them with fake traffic.

The attacks followed several computer virus outbreaks last year - such as Melissa - which spread rapidly by taking advantage of functions that were designed to make Internet use friendlier.

And last month, a hacker stole credit card numbers from the Internet music retailer CD Universe, then released thousands of them on a Web site after the firm refused to pay \$100,000 ransom.

"I fully expect the Internet to ultimately be safe and stable," said Stephen Gorrell, program manager for Norton Internet Security

### Search

the site  the Web



POWERED BY LYCOS

### Inside News

[Talk News](#)

[Nationline](#)

[Washington](#)

[World](#)

[Politics](#)

[Elections](#)

[Opinion](#)

[Columnists](#)

[Snapshot](#)

[Science](#)

[States](#)

[Weird news](#)

### Print Edition

[Today](#)

[Yesterday](#)

[Subscribe](#)

[Archive](#)



## Resources

[E-mail](#)

[Index](#)

[Feedback](#)

[What's hot](#)

[About us](#)

[Jobs at USA](#)

[TODAY](#)

## Free premiums

[USA TODAY](#)

[Update](#)

[Software](#)



software. "However, in the period of record growth, it's not surprising new holes are discovered."

The Internet's developers could not have effectively countered threats to commerce because e-businesses did not yet exist, Gorrell said.

As the Internet grows, so do the numbers of hackers and potential victims. And hackers are becoming more sophisticated, with some even developing tools to automate their attacks.

Software companies, some critics say, contribute to the problems by releasing products that still have security holes.

"Each day, technology is changing," said Robert Ing, who handles electronic security for SBR International Inc. in Toronto. "There's a rush to get products out to market because it is a competitive marketplace. Sometimes, security is overlooked."

Steve Hunt, security analyst at Giga Information Group in Chicago, hopes the latest attacks will encourage companies to take security more seriously.

"We owe quite a debt of gratitude to hackers to show us where our pants have been down," he said.

Security and Internet experts differ on how far they need to go - and that itself is a problem. Some believe in completely updating equipment and software to reduce users' anonymity and improve authentication.

In the offline world, businesses have experience with security guards and special locks. Some practices are even required by law or insurance companies.

But the Internet community has yet to agree on such standards, said Harris Miller, president of the Information Technology Association of America.

Phil Attfield, director of technical marketing at McAfee.com, said Internet security will eventually catch up.

"The approaches are going to have to become more formal rather than ad hoc," he said. "We've been getting there incrementally. That's the way technology is evolving."

But hacking will never completely disappear, said Keith Teare, the chairman and chief executive of RealNames. Vandals broke into RealNames' computers Wednesday, and the company had to warn some 20,000 customers that their credit card numbers might have been stolen.

"For every secure environment, there will be somebody prepared to try to break in," Teare said. "If they are clever enough, they will find holes."

Greg Hawkins, chief executive of Buy.com, said the attacks on his shopping site and others raised awareness.

"This is a new frontier. It's big, it's fast, and it's growing rapidly," he said. "With that growth will come continued challenges to make sure it's a secure and effective environment. We are clearly going to have growing pains like this from time to time."

- 
- [Go to Nationline](#)
  - [Go to News front page](#)
- 



Front page. [News](#). [Sports](#). [Money](#). [Life](#). [Weather](#). [Marketplace](#)

© Copyright 2000 USA TODAY, a division of Gannett Co. Inc.



You get **3** seconds  
to keep a customer online. GO .

intel.

Inter@ctive Week

April 20, 1998

## ISP Posts Blacklist Of Smurf-Friendly Networks

By Randy Barrett

One Chicago-based Internet service provider is blocking more than 40 Internet networks from its access system, until they stop allowing hackers to use bandwidth for "smurf" attacks.

Macro Computer Solutions Inc. (www.mcs.net) owner Karl Denninger posted a notice April 11 on the North American Network Operators Group e-mail list stating he was fed up with smurf attacks and would no longer exchange traffic with networks that originated the assaults.

"I'm going to start posting the blacklist here weekly in the hopes that peer pressure will cause people to clean up their acts," Denninger wrote.

Denninger listed the Internet Protocol addresses -- but not names -- of 30 networks and has added 12 more since. Most are larger Internet providers and academic networks, he said.

For network administrators, being a collaborator in a smurf attack means doing nothing at all. The attacks are often aimed at Internet Relay Chat servers or the Internet service providers (ISPs) that host them. Johnny Hacker typically gets mad at Betty Hacker during a chat session and tries to knock her offline by burning down her provider. All the assault requires is a basic Internet account.

Here's how it works: Johnny Hacker sends a stream of diagnostic "ping" messages to a second-party network's host servers. Many of those servers are set to automatically respond, but Johnny places a false return address and those responses stream to a third-party ISP that is really the target of the assault. So a single ping stream is amplified hundreds or thousands of times and clogs the target network's bandwidth -- particularly smaller providers using a single T1 (1.5-million-bit-per-second) line.

The fix is simple, Denninger said: Networks must turn off the "directed broadcast forwarding" function in their routers, and the ping responses will never be sent.

"Some of them honestly don't know about it. My response is, I'll deny you access to my network until you get your act together," he said.

Denninger's smurf amplifier blacklist is getting some support from network

### NEWS & VIEWS

[Financial News](#)  
[@ Net Index](#)  
[Web Reviews](#)  
[Columnists](#)  
[ZDNN News](#)

### RESOURCES

[Subscription Info](#)  
[Downloads](#)  
[Industry Events](#)  
[Recruitment](#)  
[Ad Marketplace](#)  
[Ad Index](#)  
[Forums](#)

### ABOUT US

[General Info](#)  
[Masthead](#)  
[Edit Calendar](#)  
[Contact Us](#)  
[Copyright](#)



administrators, but it is unclear whether any are using it to block errant networks or might be compiling their own rogues' gallery.

Jason Weisberger, chief of network operations at SoftAware Inc. in Marina del Rey, Calif., said he's not interested because a blacklist limits his own customers' connectivity. "Punitive filtering, while a good short-term fix, can create problems farther out," he said.

Denninger has been similarly zealous about the Enhanced Domain Name System ([www.edns.net](http://www.edns.net)), an alternative to InterNIC, which splintered last fall and is now in limbo.

#### Sponsored Links

---

NextCard [VISA: As low as 9.9% Fixed APR and no hidden fees!](#)

800.COM [Digital cameras priced from \\$99.94](#)

Netpliance [Discover the new one-button-access Internet Appliance](#)

News Flash [Tiny Video Camera, Color & Sound Only \\$79.99 - X10.com!](#)

Books [Save on taxes! Learn how at barnesandnoble.com!](#)

Great PCs [Buy your Dream PC at Micronpc.com. Click here!](#)

#### ZDNet Featured Links

---

Downloads [Top 50 FREE files - utilities, games, Internet & more](#)


NEW! [Shop the Outlet Store for best buys on computer products](#)

Bargains [Shop and save with FREE digital coupons and special offers!](#)

#### Magazine Offers

---

[Click Here](#) [Apply for a FREE subscription to Sm@rt Reseller](#)

	<a href="#">Reviews</a>   <a href="#">News</a>   <a href="#">Downloads</a>   <a href="#">Shop</a>   <a href="#">MyZDNet</a>   <a href="#">Games</a>   <a href="#">ZDTV</a>   <a href="#">Forums</a>
	<a href="#">AnchorDesk</a>   <a href="#">PC Magazine</a>   <a href="#">PC Week</a>   <a href="#">Help!</a>   <a href="#">Yahoo! Internet Life</a>
<b>HOME   FREE MEMBERSHIP   CONTACT ZD   AD INFO   ZIFF-DAVIS</b>	

Copyright (c) 1998 Ziff Davis, Inc. All Rights Reserved. Reproduction in whole or in part in any form or medium without express written permission of Ziff Davis, Inc. is prohibited. Inter@ctive Week and the Inter@ctive Week logo are trademarks of Ziff Davis, Inc.



Welcome to the  
Office of Senator  
Frank Murkowski

Inbox Privacy Act

North to the Future

ALASKA

HOME

For Immediate Release

## ANTI-SPAM BILL INTRODUCED TO SOLVE A NATIONAL INTERNET PROBLEM

ALASKA  
CONSTITUENT  
RESOURCES

WASHINGTON -- Senators Frank Murkowski (R-AK), Robert Torricelli (D-NJ), Conrad Burns (R-MT), and Harry Reid (D-NV) today introduced the Inbox Privacy Act to address the growing concerns of Internet consumers over the issue of junk email, or spam.

ALASKA  
LEGISLATIVE  
RESOURCES

"Internet consumers nationwide have been speaking out against the growing flood of unwanted and fraudulent e-mails in the inboxes. It's time that we had a nationwide solution to this problem. E-mail shouldn't be a way for every huckster to sell the Brooklyn Bridge," Murkowski noted.

ALASKA  
ALASKA  
RESOURCES

ALASKA  
PRESS  
RESOURCES

Senator Torricelli added, "Accessing the Internet should not be an invitation for every shyster in the world to beat down your door with junk e-mail. American consumers deserve a level of privacy and protection and our legislation provides it to them."

ALASKA  
INTERNET  
ISSUES

ALASKA  
CONTACTING  
ME

Junk e-mail burdens Internet consumers by shifting delivery costs onto consumers, particularly in rural areas like Alaska where a connection to the Internet often requires a long distance call.

The Inbox Privacy Act would require e-mail marketers to honestly identify themselves, honor consumer removal requests, and allow Internet domain owners to set up electronic "stop signs" to give domain owners the ability to block unwanted solicitations. In order to allow the Internet consumer to have the ultimate choice, unsolicited e-mails could be sent to those who still wish to receive such solicitations. Internet Service Providers, state attorney generals, and the Federal Trade Commission would have the authority to seek up to \$50,000 per day in damages.

The legislation has been referred to the Senate Commerce Committee where hearings will be held later this year. Similar legislation was passed by the Senate in the 105th Congress by a vote of 99-0 although a final conference

between the House and Senate could not be scheduled prior to adjournment.

Senator Torricelli also noted that "Our legislation continues to allow legitimate uses of e-mail, but empowers consumers and Internet service providers to eliminate the unwanted e-mail they receive."

Comments on the bill can be made to [spamfree@murkowski.senate.gov](mailto:spamfree@murkowski.senate.gov) .

---

106TH CONGRESS  
1ST SESSION

# S. 759

To regulate the transmission of unsolicited commercial electronic mail on the Internet, and for other purposes.

---

## IN THE SENATE OF THE UNITED STATES

MARCH 25, 1999

Mr. MURKOWSKI (for himself, Mr. TORRICELLI, Mr. BURNS, and Mr. REID) introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

---

## A BILL

To regulate the transmission of unsolicited commercial electronic mail on the Internet, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*  
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the "Inbox Privacy Act of  
5 1999".

6 **SEC. 2. TRANSMISSIONS OF UNSOLICITED COMMERCIAL**  
7 **ELECTRONIC MAIL.**

8 (a) **PROHIBITION ON TRANSMISSION TO PERSONS**  
9 **DECLINING RECEIPT.—**

1           (1) IN GENERAL.—A person may not initiate  
2 the transmission of unsolicited commercial electronic  
3 mail to another person if such other person submits  
4 to the person a request that the initiation of the  
5 transmission of such mail by the person to such  
6 other person not occur.

7           (2) FORM OF REQUEST.—A request under  
8 paragraph (1) may take any form appropriate to no-  
9 tify a person who initiates the transmission of unso-  
10 licited commercial electronic mail of the request, in-  
11 cluding an appropriate reply to a notice specified in  
12 subsection (d)(2).

13           (3) CONSTRUCTIVE AUTHORIZATION.—

14           (A) IN GENERAL.—Subject to subpara-  
15 graph (B), for purposes of this subsection, a  
16 person who secures a good or service from, or  
17 otherwise responds electronically to an offer in  
18 a commercial electronic mail message shall be  
19 deemed to have authorized the initiation of  
20 transmissions of unsolicited commercial elec-  
21 tronic mail from the person who initiated trans-  
22 mission of the message.

23           (B) NO AUTHORIZATION FOR REQUEST  
24 FOR TERMINATION.—A reply to a notice speci-  
25 fied in subsection (d)(2) shall not constitute au-

1           thorization for the initiation of transmissions of  
2           unsolicited commercial electronic mail under  
3           this paragraph.

4           (b) PROHIBITION ON TRANSMISSION TO DOMAIN  
5 OWNERS DECLINING RECEIPT.—

6           (1) IN GENERAL.—Except as provided in para-  
7           graph (2), a person may not initiate the trans-  
8           mission of unsolicited commercial electronic mail to  
9           any electronic mail addresses served by a domain if  
10          the domain owner has elected not to receive trans-  
11          missions of such mail at the domain in accordance  
12          with subsection (c).

13          (2) EXCEPTIONS.—The prohibition in para-  
14          graph (1) shall not apply in the case of the fol-  
15          lowing:

16                (A) A domain owner initiating trans-  
17                missions of commercial electronic mail to its  
18                own domain.

19                (B) Any customer of an Internet service  
20                provider or interactive computer service pro-  
21                vider included on a list under subsection  
22                (c)(3)(C).

23          (c) DOMAIN-WIDE OPT-OUT SYSTEM.—

1 (1) IN GENERAL.—A domain owner may elect  
2 not to receive transmissions of unsolicited commer-  
3 cial electronic mail at its own domain.

4 (2) NOTICE OF ELECTION.—A domain owner  
5 making an election under this subsection shall—

6 (A) notify the Federal Trade Commission  
7 of the election in such form and manner as the  
8 Commission shall require for purposes of sec-  
9 tion 4(e); and

10 (B) if the domain owner is an Internet  
11 service provider or interactive computer service  
12 provider, notify the customers of its Internet  
13 service or interactive computer service, as the  
14 case may be, in such manner as the provider  
15 customarily employs for notifying such cus-  
16 tomers of matters relating to such service, of—

17 (i) the election; and

18 (ii) the authority of the customers to  
19 make the election provided for under para-  
20 graph (3).

21 (3) CUSTOMER ELECTION TO CONTINUE RE-  
22 CEIPT OF MAIL.—

23 (A) ELECTION.—Any customer of an  
24 Internet service provider or interactive com-  
25 puter service provider receiving a notice under

1 paragraph (2)(B) may elect to continue to re-  
2 ceive transmissions of unsolicited commercial  
3 electronic mail through the domain covered by  
4 the notice, notwithstanding the election of the  
5 Internet service provider or interactive com-  
6 puter service provider under paragraph (1) to  
7 which the notice applies.

8 (B) TRANSMITTAL OF MAIL.—An Internet  
9 service provider or interactive computer service  
10 provider may not impose or collect any fee for  
11 the receipt of unsolicited commercial electronic  
12 mail under this paragraph (other than the  
13 usual and customary fee imposed and collected  
14 for the receipt of commercial electronic mail by  
15 its customers) or otherwise discriminate against  
16 a customer for the receipt of such mail under  
17 this paragraph.

18 (C) LIST OF CUSTOMERS MAKING ELEC-  
19 TION.—

20 (i) REQUIREMENT.—An Internet serv-  
21 ice provider or interactive computer service  
22 provider shall maintain a list of each of its  
23 current customers who have made an elec-  
24 tion under subparagraph (A).

1                   (ii) AVAILABILITY OF LIST.—Each  
2                   such provider shall make such list available  
3                   to the public in such form and manner as  
4                   the Commission shall require for purposes  
5                   of section 4(c).

6                   (iii) PROHIBITION ON FEE.—A pro-  
7                   vider may not impose or collect any fee in  
8                   connection with any action taken under  
9                   this subparagraph.

10           (d) INFORMATION TO BE INCLUDED IN ALL TRANS-  
11           MISSIONS.—A person initiating the transmission of any  
12           unsolicited commercial electronic mail message shall in-  
13           clude in the body of such message the following informa-  
14           tion:

15                   (1) The name, physical address, electronic mail  
16                   address, and telephone number of the person.

17                   (2) A clear and obvious notice that the person  
18                   will cease further transmissions of commercial elec-  
19                   tronic mail to the recipient of the message at no cost  
20                   to that recipient upon the transmittal by that recipi-  
21                   ent to the person, at the electronic mail address  
22                   from which transmission of the message was initi-  
23                   ated, of an electronic mail message containing the  
24                   word “remove” in the subject line.

1 (e) ROUTING INFORMATION.—A person initiating the  
2 transmission of any commercial electronic mail message  
3 shall ensure that all Internet routing information con-  
4 tained in or accompanying such message is accurate, valid  
5 according to the prevailing standards for Internet proto-  
6 cols, and accurately reflects the routing of such message.

7 **SEC. 3. DECEPTIVE ACTS OR PRACTICES IN CONNECTION**  
8 **WITH SALE OF GOODS OR SERVICES OVER**  
9 **THE INTERNET.**

10 (a) AUTHORITY TO REGULATE.—

11 (1) IN GENERAL.—The Federal Trade Commis-  
12 sion may prescribe rules for purposes of defining  
13 and prohibiting deceptive acts or practices in connec-  
14 tion with the promotion, advertisement, offering for  
15 sale, or sale of goods or services on or by means of  
16 the Internet.

17 (2) COMMERCIAL ELECTRONIC MAIL.—The  
18 rules under paragraph (1) may contain specific pro-  
19 visions addressing deceptive acts or practices in the  
20 initiation, transmission, or receipt of commercial  
21 electronic mail.

22 (3) NATURE OF VIOLATION.—The rules under  
23 paragraph (1) shall treat any violation of such rules  
24 as a violation of a rule under section 18 of the Fed-  
25 eral Trade Commission Act (15 U.S.C. 57a), relat-

1 ing to unfair or deceptive acts or practices affecting  
2 commerce.

3 (b) PRESCRIPTION.—Section 553 of title 5, United  
4 States Code, shall apply to the prescription of any rules  
5 under subsection (a).

6 **SEC. 4. FEDERAL TRADE COMMISSION ACTIVITIES WITH**  
7 **RESPECT TO UNSOLICITED COMMERCIAL**  
8 **ELECTRONIC MAIL.**

9 (a) INVESTIGATION.—

10 (1) IN GENERAL.—Subject to paragraph (2),  
11 upon notice of an alleged violation of a provision of  
12 section 2, the Federal Trade Commission may con-  
13 duct an investigation in order to determine whether  
14 or not the violation occurred.

15 (2) LIMITATION.—The Commission may not  
16 undertake an investigation of an alleged violation  
17 under paragraph (1) more than 2 years after the  
18 date of the alleged violation.

19 (3) RECEIPT OF NOTICES.—The Commission  
20 shall provide for appropriate means of receiving no-  
21 tices under paragraph (1). Such means shall include  
22 an Internet web page on the World Wide Web that  
23 the Commission maintains for that purpose.

24 (b) ENFORCEMENT POWERS.—If as a result of an in-  
25 vestigation under subsection (a) the Commission deter-

1 mines that a violation of a provision of section 2 has oc-  
2 curred, the Commission shall have the power to enforce  
3 such provision as if such violation were a violation of a  
4 rule prescribed under section 18 of the Federal Trade  
5 Commission Act (15 U.S.C. 57a), relating to unfair or de-  
6 ceptive acts or practices affecting commerce.

7 (c) INFORMATION ON ELECTIONS UNDER DOMAIN-  
8 WIDE OPT-OUT SYSTEM.—

9 (1) INITIAL SITE FOR INFORMATION.—The  
10 Commission shall establish and maintain an Internet  
11 web page on the World Wide Web containing infor-  
12 mation sufficient to make known to the public for  
13 purposes of section 2 the domain owners who have  
14 made an election under subsection (c)(1) of that sec-  
15 tion and the persons who have made an election  
16 under subsection (c)(3) of that section.

17 (2) ALTERNATIVE SITE.—The Commission may  
18 from time to time select another means of making  
19 known to the public the information specified in  
20 paragraph (1). Any such selection shall be made in  
21 consultation with the members of the Internet com-  
22 munity.

23 (d) ASSISTANCE OF OTHER FEDERAL AGENCIES.—  
24 Other Federal departments and agencies may, upon re-

1 quest of the Commission, assist the Commission in car-  
2 rying out activities under this section.

3 **SEC. 5. ACTIONS BY STATES.**

4 (a) **IN GENERAL.**—Whenever the attorney general of  
5 a State has reason to believe that the interests of the resi-  
6 dents of the State have been or are being threatened or  
7 adversely affected because any person is engaging in a pat-  
8 tern or practice of the transmission of electronic mail in  
9 violation of a provision of section 2, or of any rule pre-  
10 scribed pursuant to section 3, the State, as *parens patriae*,  
11 may bring a civil action on behalf of its residents to enjoin  
12 such transmission, to enforce compliance with such provi-  
13 sion or rule, to obtain damages or other compensation on  
14 behalf of its residents, or to obtain such further and other  
15 relief as the court considers appropriate.

16 (b) **NOTICE TO COMMISSION.**—

17 (1) **NOTICE.**—The State shall serve prior writ-  
18 ten notice of any civil action under this section on  
19 the Federal Trade Commission and provide the  
20 Commission with a copy of its complaint, except that  
21 if it is not feasible for the State to provide such  
22 prior notice, the State shall serve written notice im-  
23 mediately after instituting such action.

1           (2) RIGHTS OF COMMISSION.—On receiving a  
2           notice with respect to a civil action under paragraph  
3           (1), the Commission shall have the right—

4                   (A) to intervene in the action;

5                   (B) upon so intervening, to be heard in all  
6           matters arising therein; and

7                   (C) to file petitions for appeal.

8           (c) ACTIONS BY COMMISSION.—Whenever a civil ac-  
9           tion has been instituted by or on behalf of the Commission  
10          for violation of a provision of section 2, or of any rule  
11          prescribed pursuant to section 3, no State may, during  
12          the pendency of such action, institute a civil action under  
13          this section against any defendant named in the complaint  
14          in such action for violation of any provision or rule as al-  
15          leged in the complaint.

16          (d) CONSTRUCTION.—For purposes of bringing a civil  
17          action under subsection (a), nothing in this section shall  
18          prevent an attorney general from exercising the powers  
19          conferred on the attorney general by the laws of the State  
20          concerned to conduct investigations or to administer oaths  
21          or affirmations or to compel the attendance of witnesses  
22          or the production of documentary or other evidence.

23          (e) VENUE; SERVICE OF PROCESS.—Any civil action  
24          brought under subsection (a) in a district court of the  
25          United States may be brought in the district in which the

1 defendant is found, is an inhabitant, or transacts business  
2 or wherever venue is proper under section 1391 of title  
3 28, United States Code. Process in such an action may  
4 be served in any district in which the defendant is an in-  
5 habitant or in which the defendant may be found.

6 (f) DEFINITIONS.—In this section:

7 (1) ATTORNEY GENERAL.—The term “attorney  
8 general” means the chief legal officer of a State.

9 (2) STATE.—The term “State” means any  
10 State of the United States, the District of Columbia,  
11 Puerto Rico, Guam, American Samoa, the United  
12 States Virgin Islands, the Commonwealth of the  
13 Northern Mariana Islands, the Republic of the Mar-  
14 shall Islands, the Federated States of Micronesia,  
15 the Republic of Palau, and any possession of the  
16 United States.

17 **SEC. 6. ACTIONS BY INTERNET SERVICE PROVIDERS AND**  
18 **INTERACTIVE COMPUTER SERVICE PRO-**  
19 **VIDERS.**

20 (a) ACTIONS AUTHORIZED.—In addition to any other  
21 remedies available under any other provision of law, any  
22 Internet service provider or interactive computer service  
23 provider adversely affected by a violation of section  
24 2(b)(1) may, within 1 year after discovery of the violation,

1 bring a civil action in a district court of the United States  
2 against a person who violates such section.

3 (b) RELIEF.—

4 (1) IN GENERAL.—An action may be brought  
5 under subsection (a) to enjoin a violation referred to  
6 in that subsection, to enforce compliance with the  
7 provision referred to in that subsection, to obtain  
8 damages as specified in paragraph (2), or to obtain  
9 such further and other relief as the court considers  
10 appropriate.

11 (2) DAMAGES.—

12 (A) IN GENERAL.—The amount of dam-  
13 ages in an action under this section for a viola-  
14 tion specified in subsection (a) may not exceed  
15 \$50,000 per day in which electronic mail consti-  
16 tuting such violation was received.

17 (B) RELATIONSHIP TO OTHER DAM-  
18 AGES.—Damages awarded under this subsection  
19 for a violation under subsection (a) are in addi-  
20 tion to any other damages awardable for the  
21 violation under any other provision of law.

22 (C) COST AND FEES.—The court may, in  
23 issuing any final order in any action brought  
24 under subsection (a), award costs of suit, rea-  
25 sonable costs of obtaining service of process,

1 reasonable attorney fees, and expert witness  
2 fees for the prevailing party.

3 (c) VENUE; SERVICE OF PROCESS.—Any civil action  
4 brought under subsection (a) in a district court of the  
5 United States may be brought in the district in which the  
6 defendant or in which the Internet service provider or  
7 interactive computer service provider is located, is an in-  
8 habitant, or transacts business or wherever venue is prop-  
9 er under section 1391 of title 28, United States Code.  
10 Process in such an action may be served in any district  
11 in which the defendant is an inhabitant or in which the  
12 defendant may be found.

13 **SEC. 7. PREEMPTION.**

14 This Act preempts any State or local laws regarding  
15 the transmission or receipt of commercial electronic mail.

16 **SEC. 8. DEFINITIONS.**

17 In this Act:

18 (1) **COMMERCIAL ELECTRONIC MAIL.**—The  
19 term “commercial electronic mail” means any elec-  
20 tronic mail or similar message whose primary pur-  
21 pose is to initiate a commercial transaction, not in-  
22 cluding messages sent by persons to others with  
23 whom they have a prior business relationship.

24 (2) **INITIATE THE TRANSMISSION.**—

1 (A) IN GENERAL.—The term “initiate the  
2 transmission”, in the case of an electronic mail  
3 message, means to originate the electronic mail  
4 message.

5 (B) EXCLUSION.—Such term does not in-  
6 clude any intervening action to relay, handle, or  
7 otherwise retransmit an electronic mail mes-  
8 sage, unless such action is carried out in inten-  
9 tional violation of a provision of section 2.

10 (3) INTERACTIVE COMPUTER SERVICE PRO-  
11 VIDER.—The term “interactive computer service  
12 provider” means a provider of an interactive com-  
13 puter service (as that term is defined in section  
14 230(c)(2) of the Communications Act of 1934 (47  
15 U.S.C. 230(c)(2)).

16 (4) INTERNET.—The term “Internet” has the  
17 meaning given that term in section 230(c)(1) of the  
18 Communications Act of 1934 (47 U.S.C. 230(c)(1)).

○

**HB**

**404**



# ALASKA STATE LEGISLATURE

REPRESENTATIVE GARY DAVIS

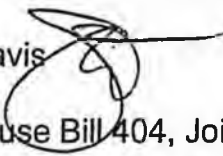
RECEIVED

APR 07 2000

April 7, 2000

## MEMORANDUM

TO: Representative Norm Rokeberg, Chair  
House Labor and Commerce Committee

FRC #1: Representative Gary Davis 

RE: Hearing Request for House Bill 404, Joint Insurance Arrangements

Please schedule a hearing for House Bill 404, "An Act relating to joint insurance arrangements; and providing for an effective date," at your convenience.

Attached are the following for inclusion in the committee packet

- sponsor statement
- Zero fiscal note from Department of Community & Economic Development
- AS 21.76.010 - 120, Joint Insurance Arrangements
- AS 29.24.010 listing the general powers of municipalities
- AS 21.12.030 - 112 defining types of insurance
- position paper by the Alaska Municipal League Joint Insurance Association in support of the legislation,
- list of the Fiscal Year 2000 participants in the association
- letters of support from the cities of Kotzebue, Seward and Soldotna, the South Naknek Village Council, Kotlik Traditional Council, and Ugashik Traditional Village

Also attached is a position paper by the Alaska Independent Insurance Agents and Brokers, Inc. opposing HB 404. A response to this opposition with possible amendments to alleviate their concerns follows. I leave it to your discretion as to whether or not to offer these amendments.

Thank you for your consideration of this request. If you have any questions or would like additional information, please contact Deb Davidson of my staff.

RECEIVED

APR 07 2000



# ALASKA STATE LEGISLATURE

REPRESENTATIVE GARY DAVIS

## SPONSOR STATEMENT Committee Substitute to House Bill 404 (C&RA)

*An Act relating to joint insurance arrangements and providing for an effective date*

House Bill 404 amends AS 21.76.010(a) to expand the types of entities allowed to enter into joint insurance arrangements for the purpose of assuming risks from losses or purchasing coverage. Native village councils, Native associations and nonprofit corporations could enter into these agreements provided that the council, association or corporation exercises at least two of the general municipal powers described under AS 29.35.010 and either a municipality, municipal corporation, school district or REAA is also a member of the agreement.

Unincorporated communities in which Native councils, Native associations or small nonprofit corporations exercise traditional governmental functions have trouble obtaining affordable insurance coverage in the traditional market. Small, nonprofit corporations such as friends of the library, senior citizen centers and other organizations within municipalities also experience this difficulty.

House Bill 404 would allow these entities to enter into the cooperative agreements currently enjoyed by organized municipalities in Alaska. They would be able to obtain the needed insurance at a more affordable rate provided to larger insurance pools and by sharing the risk for potential losses.

In order to qualify for the ability to enter into an agreement, the nonprofit corporation, or the Native association or village council would need to exercise at least two of the general powers given to organized municipalities in the state. Additionally, a municipality, municipal corporation, school district or REAA would also have to be a member of the agreement.

Joint insurance agreements may be entered into for the following types of insurance coverage: disability, property, casualty, surety, marine, wet marine and transportation and mortgage guaranty. It may not be entered into for health, life or title insurance purposes.

This legislation was requested by the Alaska Municipal League/Joint Insurance Association and has the support of their umbrella organization, the Alaska Municipal League as well.

# FISCAL NOTE

**STATE OF ALASKA**  
**2000 LEGISLATIVE SESSION**

**BILL NO. HB 404**

Revision Date/Time (Note if correction) \_\_\_\_\_ Dept. Affected Community & Economic Development  
 Title An Act relating to joint insurance arrangements; BRU Insurance  
 and providing for an effective date. \_\_\_\_\_ Component Insurance  
 Sponsor Representative Davis  
 Requester House CRA Component No. 354

**Expenditures/Revenues** (Thousands of Dollars)

Note: Amounts do not include inflation unless otherwise noted below.

OPERATING EXPENDITURES	FY 2001	FY 2002	FY 2003	FY 2004	FY 2005	FY 2006
Personal Services						
Travel						
Contractual						
Supplies						
Equipment						
Land & Structures						
Grants & Claims						
Miscellaneous						
<b>TOTAL OPERATING</b>	<b>0.0</b>	<b>0.0</b>	<b>0.0</b>	<b>0.0</b>	<b>0.0</b>	<b>0.0</b>

<b>CAPITAL EXPENDITURES</b>						
-----------------------------	--	--	--	--	--	--

<b>CHANGE IN REVENUES ( )</b>						
-------------------------------	--	--	--	--	--	--

**FUND SOURCE** (Thousands of Dollars)

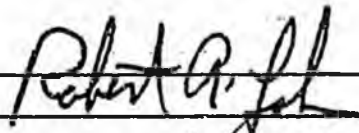
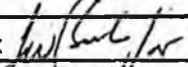
1002 Federal Receipts						
1003 GF Match						
1004 GF						
1005 GF/Program Receipts						
1037 GF/Mental Health						
Other (Specify Type)						
<b>TOTAL</b>	<b>0.0</b>	<b>0.0</b>	<b>0.0</b>	<b>0.0</b>	<b>0.0</b>	<b>0.0</b>

Estimate of any current year (FY2000) cost: \_\_\_\_\_

**POSITIONS**

Full-time						
Part-time						
Temporary						

**ANALYSIS:** (Attach a separate page if necessary)  
 No fiscal on this component.

Prepared by: Robert A. Lohr  Phone 269-7900  
 Division Insurance Date/Time 3-20-00 9:03 AM  
 Approved by Commissioner Deborah B. Sedwick  Date 3-20-00  
 Agency Community & Economic Development

**PREPARER TO PROVIDE ALL DISTRIBUTION COPIES TO GOVERNOR'S LEGISLATIVE OFFICE**  
 For further distribution information, call the Governor's Legislative Office



907 G Street, Suite 358  
Anchorage, Alaska 99501  
(907) 256-2625  
(907) 279-3816 Fax  
1-800-337-3882 toll free in Alaska

ANCHORAGE OFFICE

## POSTION PAPER

The Alaska Municipal League Joint Insurance Association (AML/JIA) supports changes to AS 21.76 adding small nonprofits, Native associations, and Native village governments to the existing pooling statute.

Each month, the AML/JIA receives phone calls from Native village governments seeking insurance coverage. They are disappointed to discover that this is permitted for municipal governments organized under state law, but not for the 227 Federally recognized Native village governments in Alaska. Apparently, they have had some trouble finding coverage in the traditional market.

It is also common to hear from our member municipalities or school districts that are seeking coverage for small-nonprofit partners such as friends of the library, senior citizen centers, the humane society (animal control) or others who perform traditional governmental functions.

It is the AML/JIA's view that as state aid to municipalities declines, more services are being dropped or shifted to other service providers. Since existing pools organized under AS21.76 are accustomed to dealing with these exposures, it makes sense to permit these entities to pool with the new service providers as well.

A number of municipalities have dissolved in the past six years, and many more are seriously questioning their future. In many of these cases, especially where municipal governments have already dissolved, Native village governments have stepped in to provide services.

Since the *Venette* decision, it seems clear that these Native village governments in Alaska do not have taxing authority over non-members in the absence of Indian Country. This lack of taxing authority is a concern for some, who feel that state-organized municipalities with taxing authority could be paying for losses in small communities without taxing authority in the unlikely event of a pool failure. This is already the case.

Page 1 of 3

February 9, 2000  
AML/JIA Position Paper

Many small communities such as Platinum (52) may have the authority to tax, but without a tax base they are essentially in the same position as Native village governments. This one reason why Alaska's pools have structured themselves to use excess insurance or reinsurance to avoid the catastrophic losses that could threaten a pool's financial integrity. The assessment provisions presently in statute were placed there to provide a level of comfort to the lawmakers of the mid-80's when the pooling concept was still a new idea. As a practical matter, it would be financial suicide for a pool to assess a member (possibly requiring them to go back to the taxpayers). This has never happened and is essentially a safety valve that fourteen years after the initial law was passed seems inconceivable to use.

In fact, the tax issue would only arise if all a pool's assets were insufficient to fund a loss. The AML/JIA presently exceeds all national pooling standards by a significant margin, and has admitted assets of approximately \$18 million. Since the AML/JIA is never exposed to more than \$250,000 on any loss it would take more large losses in a single year than we have experienced in the past 12 years total to exhaust the financial resources of the organization.

The Alaska Municipal League (AML) also supports the idea of adding Native village governments to the pooling statute. The 2000 Policy Statement (Local Govt. Powers, D, 2) states:

*2. Risk-Pooling: The League supports legislation enabling tribal organizations that provide municipal services to pool for the purposes of risk sharing and insurance services. As state funds to municipalities decline, tribal entities are filling the void to provide municipal-type services to Alaska's citizens. Pooling is a cost-effective, efficient method for handling insurance needs of all entities providing these critical public services. Amending AS 21.76 to permit tribal organizations to pool with municipalities helps keep the cost of providing public services lower. (am 11/99)*

In summary, both the AML & the AML/JIA support the idea of amending AS21.76 to include groups such as nonprofits and Native village governments providing municipal services. In fact, it is important to note that in the absence of a municipal government, the State of Alaska may be

FROM : GILLESPIE & ASSOCIATES  
FEB-09-00 WED 01:31 PM AML/JIA

PHONE NO. : 907 463 5522  
FAX NO. 907 210 3012

Feb. 09 2000 03:18PM P4  
11 03/00

February 9, 2000  
AML/JIA Position Paper

facing liabilities associated with the public infrastructure such as schools. As public sector services in Alaska continue to shift to different public sector service providers, the need for affordable coverage and loss control services continues to be an important issue. Alaska's public entity pools seem a logical mechanism to provide affordable, quality risk financing to protect municipalities, Native village government organizations, small nonprofits, and the State of Alaska's citizens.

If I can answer any questions regarding this proposal, please let me know.

Sincerely,



Eileen Terwilliger, ARM  
Executive Director  
AML/JIA

---

**Alaska Municipal League Joint Insurance Association, Inc.**

---

**FY2000 Participants**

51 Akhiok	117 Gambell	63 Nuiqsut
7 Akutan	4 Golovin	85 Nulato
89 Alakanuk *	60 Goodnews Bay	146 Nunapitchuk
86 Aleknagik	133 Haines *	53 Old Harbor
82 Aleutians East Borough	134 Haines Borough/Schools	19 Ouzinkie
88 Aleu. East Boro Schools	157 Homer - <i>PI</i>	20 Palmer *
118 Ambler	160 Hoonah - <i>SG</i>	57 Pelican
147 Anch.SD/Aquarian Chtr - <i>WC</i>	67 Hoonah Schools	72 Pilot Point
148 Anch.SD/FamilyPartnership Chtr - <i>WC</i>	13 Hooper Bay	43 Pilot Station
164 Anch.SD/Village Chtr - <i>WC</i>	41 Houston	98 Platinum
149 Anch.SD/Walden Chtr - <i>WC</i>	130 Hughes	68 Point Hope
99 Anderson	31 Huslia	119 Port Alexander
55 Aniak	84 Hydaburg	144 Port Heiden - <i>BLA</i>
81 Anvik	124 Iditarod Area Schools - <i>RL</i>	23 Port Lions
46 Atka	153 Kaktovik	156 Pribilof School District - <i>WC</i>
50 Atkasuk	107 Kaltag	163 Ruby/Ruby Electric - <i>WC</i>
10 Barrow	69 Kasaaan	59 Russian Mission
95 Bethel * - <i>RL</i>	154 Kenai Pen. Boro/Schools	77 St. George
100 Bettles	48 Kiana	32 St. Mary's *
101 Brevig Mission	38 King Cove *	137 St. Mary's Schools - <i>RL</i>
74 Bristol Bay Borough/Schools *	56 Klawock *	145 St. Michael
91 Buckland	78 Kobuk	35 Sand Point*
103 Cheifmak	93 Kodiak * - <i>B</i>	108 Savoonga
104 Chevak	102 Kodiak Island Borough/Schools	106 Saxman
80 Chignik	39 Kotlik	83 Scammon Bay
37 Chuathbaluk	15 Kotzebue *	96 Selawik
167 Clark's Point	165 Koyuk	138 Seldovia - <i>PI</i>
112 Coffman Cove	155 Koyukuk	34 Seward *
47 Cola Bay	114 Kuspuk Schools	152 Nunam Iqua
131 Copper River Schools - <i>RL</i>	158 Kwethluk *	1 Soldotna *
159 Cordova/Schools/Medical Ctr. * - <i>B</i>	97 Lake & Peninsula Borough	162 SW Region School District - <i>B</i>
66 Craig Schools	62 Larsen Bay	94 Tanana
52 Deering	71 Lower Kalskag	161 Tanana School District - <i>WC</i>
141 Delta Junction - <i>WC</i>	136 Lower Yukon Schools - <i>RL</i>	58 Teller
90 Denali Borough	168 Manokotak	27 Tenakee Springs
36 Dillingham *	128 Marshall *	28 Thorne Bay
109 Dillingham Schools	110 McGrath	65 Togiak *
105 Diomede	16 Mountain Village *	8 Unalakleet *
11 Eagle	2 Nenana *	122 Valdez (LELP)* - <i>WC</i>
70 Eek	121 Nenana City Schools - <i>WC</i>	6 Wainwright
113 Egcgik *	166 New Stuyahok	79 Wasilla *
151 Ekwok	45 Newhalen	49 White Mountain
12 Elim	17 Nikolai	21 Whittier *
5 Emmonak *	33 Nome *	116 Wrangell *
61 False Pass	42 Noorvik	76 Yakutat, City & Borough *
73 Fort Yukon *	169 North Pole (LELP)* - <i>WC</i>	139 Yakutat Schools - <i>SG</i>
142 Galena * - <i>WC</i>	150 North Slope Borough (LELP)* - <i>B</i>	140 Yukon Flats Schools - <i>WC</i>
		138 CORE Participants
		3 LELP only
		<hr/> <b>141 Total Participants</b> <hr/>



P.O. Box 46  
Kotzebue, Alaska 99752

City Hall  
442-3401

Police Dept.  
442-3351

Fire Dept.  
442-3401

Public Works  
442-3401

February 29, 2000

Rep. Gary Davis  
Room 513  
State Capitol  
Juneau, Alaska 99801-1182

Dear Rep. Davis:

As you are well aware, municipal governments and schools are experiencing extreme financial pressures, particularly in Rural Alaska. Many of the smallest cities are on the brink of dissolution. Regardless of the size of the community, some of the services have been and are being out-sourced to local Native organizations or non-profits, such as the library, animal control, museums, senior citizen centers, and even plowing roads in some communities.

As a member of the Alaska Municipal League/Joint Insurance Association's pooling arrangement, the City of Kotzebue has, as have all other pool members, been fortunate to having good insurance coverage for the services we provide at reasonable rates. Our concern is that as we transfer municipal services to non-profits or Native Village groups, that those entities be allowed to utilize the same sound and proven mechanism for securing good insurance coverage at reasonable rates so that our constituency is protected.

Adequate insurance protection at reasonable rates in Rural Alaska is difficult to obtain. As more and more small cities drop the services that have been funded by the State and local Native village governments take over those services, the State of Alaska shares in the liability for those functions. Having adequate insurance protection serves to protect the State's interests as well.

Therefore we are very supportive of HB404. If there are any questions we can answer, please do not hesitate to call.

Sincerely,

Nancy E. Gastad  
City Manager

**CITY OF SEWARD**  
P.O. BOX 167  
SEWARD, ALASKA 99664-0167



- Main Office (907) 224-4050
- Police (907) 224-3338
- Harbor (907) 224-3138
- Fire (907) 224-3445
- Fax (907) 224-4038

March 13, 2000

Representative Gary Davis  
Room 513  
State Capitol  
Juneau, Alaska 99801-1182

Dear Representative Davis:

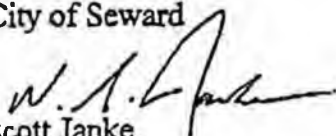
As you are aware, municipal governments and school districts are experiencing financial pressures, particularly in rural Alaska. Many of the smallest cities are on the brink of dissolution. Regardless of the size of the community, some of the services have been and are being out-sourced to local Native organizations or non-profits, such as the library, animal control, museums, senior citizen centers and even plowing roads in some communities.

As a member of the Alaska Municipal League Joint Insurance Association's pooling arrangement, the City of Seward has, as have all other pool members, been fortunate to have good insurance coverage for the services we provide at reasonable rates. Our concern is that as we transfer municipal services to non-profits or Native Village groups, that those entities be allowed to utilize the same sound and proven mechanism for securing good insurance coverage at reasonable rates so that our constituency is protected.

Adequate insurance protection at reasonable rates in rural Alaska is difficult to obtain. As more and more small cities drop the services that have been funded by the State and local Native Village governments and/or non-profit organizations take over those services, the State of Alaska shares in the liability for those functions. Having adequate insurance protection serves to protect the State's interests as well.

Therefore we are very supportive of HB404.

Sincerely,  
City of Seward

  
Scott Janke,  
City Manager

Phone: 907-224-4047  
Fax: 907-224-4038  
E-mail: [citymgr@seward.net](mailto:citymgr@seward.net)

rlg

# City of Soldotna

177 North Birch • Soldotna, Alaska 99669 • Phone: (907) 262-9107



To HB404  
File (DEC)  
JL

March 17, 2000

The Honorable Gary Davis  
House of Representatives  
State Capitol  
Room 513  
Juneau, Alaska 99801-1182

Dear Representative Davis:

The City of Soldotna is a charter member of the Alaska Municipal League/Joint Insurance Association and as such fully support HB404 which would allow the AML/JIA risk pool to expand to include Native associations, Native village councils and non-profits exercising at least two municipal powers as listed in AS 29.35.010.

It is our belief that adding these entities will make the pool stronger, as well as provide the needed affordable coverage and loss control services to those who are now attempting to provide such items even though they are not part of a municipality.

We support HB404 as the best way to provide them with coverage while hopefully lowering the cost of providing public services for us all.

Sincerely,

A handwritten signature in cursive script, appearing to read "Ken Lancaster".

Ken Lancaster  
Mayor

**Subject: Fw: HB 404**

**Date:** Mon, 6 Mar 2000 11:54:14 -0900

**From:** "Kevin Smith" <kev@pobox.alaska.net>

**Reply-To:** "Kevin Smith" <kevins@jnu.amljia.org>

**To:** "Rep. Gary Davis" <Representative\_Gary\_Davis@legis.state.ak.us>

**CC:** "Deb Davidson" <Deb\_Davidson@legis.state.ak.us>, <ftasnvc@bristolbay.com>

Dear Rep. Davis:

I received this e-mail of support for HB404 that you might wish to add to your growing collection.

-- Kevin Smith

----- Original Message -----

From: [ftasnvc](mailto:ftasnvc)

To: [kevins@jnu.amljia.org](mailto:kevins@jnu.amljia.org)

Sent: Monday, March 06, 2000 11:03 AM

Subject: HB 404

The South Naknek Village Council supports passage of HB 404. We are a federally recognized tribe and have been providing services to all community members since our inception in the early 60's. Although we are part of the Bristol Bay Borough, we provide our own water and sewer, health services and federal and state grants.

We support HB 404 since it would lower our insurance premiums.