INTRUSION INC
Form 10-K
March 26, 2004

UNITED STATES

SECURITIES AND EXCHANGE COMMISSION

WASHINGTON, D.C. 20549

FORM 10-K

(Mark One)

ý **ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934 [FEE REQUIRED]**

FOR THE FISCAL YEAR ENDED DECEMBER 31, 2003

OR

o **TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934 [NO FEE REQUIRED]**

For the transition period from to

COMMISSION FILE NUMBER 0-20191

Intrusion Inc.

(Exact name of registrant as specified in its charter)

DELAWARE	**75-1911917**
(State or other jurisdiction of incorporation or organization)	(I.R.S. Employer Identification No.)

1101 EAST ARAPAHO ROAD
RICHARDSON, TEXAS **75081**
(Address of principal executive offices) (Zip Code)

Registrant s telephone number, including area code: **(972) 234-6400**

Securities registered pursuant to Section 12(b) of the Act:

None

Securities registered pursuant to Section 12(g) of the Act:

Common Stock, $0.01 par value

(Title of class)

Indicate by check mark whether the Registrant (1) has filed all reports required to be filed by Section 13 or 15(d) of the Securities Exchange Act of 1934 during the preceding 12 months (or for such shorter period that the Registrant was required to file such reports), and (2) has been subject to such filing requirements for the past 90 days. Yes ý No o

Indicate by check mark if disclosure of delinquent filers pursuant to Item 405 of Regulation S-K is not contained herein, and will not be contained, to the best of the Registrant s knowledge, in definitive proxy or information statements incorporated by reference in Part III of this Form 10-K or any amendment to this Form 10-K. o

Indicate by check mark whether the Registrant is an accelerated filer (as defined in Exchange Act Rule 12-b2): Yes o No ý

State the aggregate market value of the voting and non-voting equity held by non-affiliates computed by reference to the price at which the common equity was last sold, or the average bid and asked price of such common equity, as of the last business day of the Registrants most recently completed second fiscal quarter: $10,381,910. As of February 27, 2004, 20,652,425 shares of the Registrant s Common Stock were outstanding.

DOCUMENTS INCORPORATED BY REFERENCE

Portions of the Registrant s definitive Proxy Statement filed in connection with the Registrant s 2003 Annual Meeting of Stockholders are incorporated by reference into Part III of this Form 10-K.

INTRUSION INC.

INDEX

PART I

Item 1. Business.

In addition to the historical information contained herein, the discussion in this Form 10-K contains certain forward-looking statements, within the meaning of Section 27A of the Securities Act of 1933 and Section 21E of the Securities Exchange Act of 1934, that involve risks and uncertainties, such as statements concerning: growth and anticipated operating results, developments in our markets and strategic focus; new products and product enhancements; potential acquisitions and the integration of acquired businesses, products and technologies; strategic relationships and future economic and business conditions. The cautionary statements made in this Form 10-K should be read as being applicable to all related forward-looking statements whenever they appear in this Form 10-K. Our actual results could differ materially from the results discussed in the forward-looking statements. Factors that could cause or contribute to such differences include, but are not limited to, those discussed under the section captioned Factors That May Affect Future Results of Operations in Item 1 of this Form 10-K as well as those cautionary statements and other factors set forth elsewhere herein.

General

We develop, market and support a family of network intrusion prevention and detection systems and regulated information compliance systems that address vital security issues facing organizations with mission critical business applications or housing classified, confidential, or customer information assets. We currently provide network security and regulated information compliance solutions under our SecureNet family of hardware and software solutions.

We market and distribute our products through a direct sales force to end-users, distributors and by numerous domestic and international system integrators, managed service providers and value-added resellers. Our end-user customers include high technology, manufacturing, telecommunications, retail, transportation, health care, insurance, entertainment, utilities and energy companies, government agencies, financial institutions, and academic institutions.

We were organized in Texas in September 1983 and reincorporated in Delaware in October 1995. For more than 15 years, we provided local area networking equipment and were known as Optical Data Systems or ODS Networks. On April 17, 2000, we announced plans to sell, or otherwise dispose of, our networking divisions, which included our Essential Communications division (Essential) and our local area networking assets. In accordance with these plans, we have accounted for these businesses as discontinued operations. On June 1, 2000, we changed our name from ODS Networks, Inc. to Intrusion.com, Inc., and our NASDAQ ticker symbol from ODSI to INTZ to reflect our focus on intrusion detection solutions. On November 1, 2001, we changed our name from Intrusion.com, Inc. to Intrusion Inc.

Our principal executive offices are located at 1101 East Arapaho Road, Richardson, Texas 75081, and our telephone number is (972) 234-6400. Our website URL is www.intrusion.com. References to we , us , our or Intrusion Inc. refer to Intrusion Inc. and its subsidiaries.

Recent Developments

On March 25, 2004, we completed a $5.0 million private placement of 5% Convertible Preferred Stock and warrants. In the private placement, the company sold 1,000,000 shares of preferred stock at a price of $5.00 per share, which convert into 6,361,323 shares of common stock at an initial conversion price of $0.786 per share, and warrants to purchase 2,226,459 shares of common stock at an exercise price of $0.786 per share. In connection with the closing of this private placement, we issued warrants to purchase 257,633 shares of our common stock at an exercise price of $0.786 per share to our financial advisor for the private placement.

On March 18, 2004, at a special meeting, our stockholders approved an amendment to our certificate of incorporation to effect a four-for-one (4:1) reverse stock split of our common stock. The reverse stock split will become effective on March 29, 2004. All outstanding share numbers and related common stock numbers, such as earnings per share and outstanding options, included in this report are set forth on a pre-split basis.

Industry Background

In the last decade, network security has changed from being a technology deployed only by the government and the most sophisticated or most paranoid of companies, to technology employed by all sizes of business and a mandatory component of all mission critical systems. This change has come about with the permeation of the Internet as a business enabler. Today, email, instant messengers, World Wide Web access, web sites, web-based applications and e-commerce are integral components of communications and operations for business and government.

Although the Internet has many business advantages, its openness and accessibility makes it a potential threat to the networks and systems that are attached to it. Computer hackers, curious or disgruntled employees, competitors and innocent mistakes may compromise or destroy information assets or disrupt the normal operations and brand equity of the enterprise.

Enterprises are adopting a variety of security solutions to meet the challenge posed by external and internal threats. To be effective, organizations require enterprise-wide information risk management solutions that are broadly deployed and centrally managed. Organizations seek systems with the optimum combination of best-of-breed capabilities and total cost of ownership. Securing the enterprise network requires two key elements:

Control: the ability to affect network traffic including access to the network or parts thereof in order to enforce a security policy.

Visibility: the ability to see and understand the nature of the network and the traffic on the network, which assists in decision making as well as crafting and constant improvement of a security policy.

We focus on providing these two primary ingredients of network security within a single device for overall network security and for the protection of specific classified, confidential or customer information assets.

Network Intrusion Prevention and Detection Systems

Network Intrusion Prevention & Detection Systems (NIP&DS) analyze network traffic for attacks and can block threats from entering the network. They examine individual packets within the data stream to identify threats from authorized users, back-door attacks and hackers who have thwarted the firewall to exploit network connections, cause system outages and access information assets. NIP&DS provide insight into the nature and character of the network that can be used to:

Identify threats in real time and block or terminate offending communications or simply alert administrators so that human intervention can protect the network;

Increase the value and efficacy of the control systems like firewalls and routers with evidence of the efficacy of those systems; and

Provide decision support for the altering of the enterprise security policy and network management.

Regulated Information Compliance Systems

Regulated Information Compliance Systems (RICS) build upon NIP&DS with the added capability to more deeply analyze traffic searching for classified, confidential or customer information assets. Working under the same management and monitoring umbrella of NIP&DS, RICS address data confidentiality, security and integrity issues facing industries subject to the Health Portability and Accountability Act of 1996 (HIPAA), Gramm, Leach, Bliley Act (GLBA), Sarbanes-Oxley, California Senate Bill 1386 (CA SB 1386) and others. These laws affect a broad range of both private and public entities, including those that maintain information that can personally identify a customer or patient and those that house both classified and unclassified information. Penalties for non-compliance include fines, lawsuits, and business process reviews.

Our Solution and Products

Intrusion Inc. addresses the challenges of ensuring the confidentiality, security and integrity of electronic information assets by developing, marketing and supporting a family of NIP&DS and RICS for deployment by public and private enterprises, to include remote and branch offices, and for managed security service providers. We believe implementing adequate perimeter defenses and monitoring network traffic to trust-but-verify are critical elements for the protection of information assets and integrity.

Our SecureNet Network Systems

The Intrusion SecureNet System has two primary components, Sensors and the Management System.

Sensors are devices or software components that are connected to the network and monitor the traffic searching for matches to signatures as evidence of an external network attack or malicious use that could threaten information assets. Signatures are patterns, anomalies and traffic flows that match known attacks or indicate suspicious activities. When the Sensor matches traffic to a signature it will send an event to the Management System.

The Management System controls the Sensors and displays events produced by the Sensors. Management is used for both configuration of the system and providing highly productive monitoring of the events produced by the system. Management is typically three-tier, where Sensors report to a centralized management system that has multiple analysts viewing the data. Management can also be a standalone system for small- and medium-businesses where configuration and monitoring are all done directly from the Sensor.

We have simplified deployment, management and monitoring to reduce the total cost of ownership for an easy to set up and manage enterprise system. To reduce barriers and provide complete enterprise integration, the Intrusion SecureNet system provides more customization and event flow options for high-end deployments.

Our SecureNet system is plug-and-protect and can be connected to any network without interfering with the network operations by using the Intrusion SecureNet passive and inline taps.

Intrusion SecureNet NIP&DS Products

We believe a primary advantage of the SecureNet NIP&DS is that with a single license purchase, the consumer may choose to deploy the system for intrusion prevention or intrusion detection, providing a superior level of flexibility and simple migration from passive detection to active prevention without additional licensing cost.

Network Intrusion Prevention Systems (NIPS) Provide network monitoring and analysis functionality like an IDS, with the added ability to block malicious network traffic. IPS actively regulates inbound and outbound traffic based on specific users access while controlling what they can do with that access on a granular, per-conversation basis.

Network Intrusion Detection Systems (NIDS) Provide detection of specific exploit and misuse patterns in the traffic that the firewall allows. IDS detect known exploits and misuse patterns, suspicious activities and anomalous traffic or behavior within both inbound and outbound traffic. This added visibility provides a checking mechanism for the efficacy of the firewall s rule base.

Intrusion SecureNet network NIP&DS provide user customizable, protocol decode detection technology for up to Gigabit networks. While Intrusion SecureNet Sensors are in the top-tier of the market for detection and throughput technology, we believe one of the primary benefits provided by our NIP&DS products is to reduce the total cost of ownership to our customers.

The SecureNet NIP&DS product family provides intuitive and powerful data mining and configuration. Intrusion SecureNet Provider is the three-tier enterprise management and monitoring system. SecureNet Provider is for enterprise deployments with no license limitations placed on architecture, freeing the enterprise to build the management system required. SecureNet Provider follows the workflow of the security analyst with a highly productive environment for response, research, resolution and decision support. The SecureNet Provider suite includes applications for event monitoring, policy creation and tuning and centralized software deployment making up the complete suite of tools required to manage and monitor a SecureNet System from five sensors to more than 100.

Our SecureNet Sensors have their own web browser interface for effortless configuration. SecureNet Sensors also deliver complete, stand-alone NIP&DS for the small and medium business with local management and monitoring. This allows customers to use their standard web browser to access a full power; full-features network NIP&DS, without additional hardware or software.

Our SecureNet NIP&DS Sensors are available as Software-Appliances and Hardware-Appliances with performance and pricing appropriate for networks ranging from 10Mb/s to Gigabit with a Common Criteria EAL2 certified Gigabit appliance. The following is a list of our IPS and IDS products

Intrusion SecureNet 7000 Software-Appliance products for networks up to 1000Mb/s. Seamlessly turns leading servers and workstations into SecureNet Sensors.

Intrusion SecureNet CC 7345 rack mount Hardware-Appliance, highly redundant, gigabit Sensor with Common Criteria EAL2 certification specifically for government deployments.

Intrusion SecureNet 7145 rack mount, gigabit Hardware-Appliance available with either a copper- or a fiber-monitoring interface.

Intrusion SecureNet 5500 Software-Appliance for networks up to 250Mb/s. Seamlessly turns leading servers and workstations into SecureNet Sensors.

Intrusion SecureNet 5545 rack mount 250Mb/s Hardware-Appliance for server rooms and datacenters.

Intrusion SecureNet 5000 Software-Appliance for networks up to 100Mb/s. Seamlessly turns leading servers and workstations into SecureNet Sensors.

Intrusion SecureNet 5445 rack mount and 2445 desktop 100Mb/s Hardware-Appliances for network deployments and remote and branch offices.

Intrusion SecureNet 2000 Software-Appliance for networks up to 10Mb/s. Seamlessly turns leading servers and workstations into SecureNet Sensors.

Intrusion SecureNet 2245 Hardware-Appliance for remote and branch offices with throughput up to 10Mb/s at about the price of a laptop.

Intrusion SecureNet RICS Products

RICS provide protection against the loss and misuse of regulated, classified and commercially sensitive data. Loss of information assets that contain customer data has spawned a multitude of federal and state legislation to set a standard of care, use and protection for customer information. Better known laws that regulate customer information include HIPAA, Gramm-Leach-Bliley Act and its UK equivalent Privacy Act of 1998, and California SB 1386. Penalties for non-compliance include fines, lawsuits, imposed processes and enforced business limitations. Any enterprise that falls within the scope of these laws is now working under a timeline to demonstrate compliance. In addition, both government and commercial institutions are becoming increasingly concerned about the misuse and loss of classified or commercially sensitive data, and are seeking proactive solutions to deal with these issues.

The Intrusion SecureNet RICS products leverage the same Management and Sensor components of the SecureNet NIP&DS products. Our SecureNet RICS solutions are currently designed to address the security and confidentiality issues in the following industries and customers:

Department of defense to help prevent the leakage of classified information,

Health care companies (including health care providers, insurance companies and medical equipment manufacturers) who are working to comply with HIPAA, and

Financial institutions and e-commerce enterprises working to comply with the customer confidentiality provisions of GLBA and CA SB 1386.

The Intrusion SecureNet RICS products leverage the same Management and Sensor components of the SecureNet IDS AND IPS products. The SecureNet RICS is designed to address the [privacy, confidentiality and information security] concerns of the department of defense, health care vertical (including health care providers, insurance companies and medical equipment manufacturers), financial institutions and e-commerce.

SecureNet RICS solutions provide accuracy through our Dynamic Data Dictionary (D3) technology, which securely connects directly to a database housing the confidential, classified, or regulated information. The RICS stays up to date with the database to match network traffic to the information that is resident in the database. This provides an automated accurate mechanism to identify leaks and misuse of information assets.

The Intrusion SecureNet LPS, leak prevention system targets public and private enterprises with confidential and classified information. The first release specifically targets the U.S. department of defense and protecting against spillage , when classified information leaks to unclassified networks.

Third-Party Products

We believe that it is beneficial to work with third parties with complementary technologies to provide integrated solutions to our customers. As there is rapid technological advancement and significant consolidation in the network security industry, there can be no assurance that we will have access to all of the third-party products that may be desirable or for the term desirable to offer fully integrated solutions to our customers.

Customer Services

In addition to offering our network security products, we also offer a wide range of services, including design and configuration, project planning, training, installation and maintenance.

Product Development

The network security industry is characterized by rapidly changing technology, standards, economy and customer demands. We believe that our future success depends in large part upon the timely enhancement of existing products as well as the development of technologically advanced new products that meet industry standards, perform successfully and simplify the user s tasks so that they can do more with less resources, all to achieve market acceptance. We are currently marketing next-generation network NIP&DS products and RICS products and are developing products to meet emerging market requirements and are continuously engaged in testing to ensure that our products interoperate with other manufacturers products, which comply with industry standards.

During 2003, 2002 and 2001, our research and development expenditures were $3.5 million $6.1 million, and $12.5 million, respectively. All of our expenditures for hardware and software research and development costs have been expensed as incurred. At December 31, 2003, we had 15 employees engaged in research and product development.

Manufacturing and Supplies

Our operational strategy relies on the outsourcing of manufacturing components, assembly and certain other operations to reduce fixed costs and to provide flexibility in meeting market demand.

Our internal manufacturing operations consist primarily of replication of software on CDs, packaging, testing and quality control of finished units. Materials used in our manufacturing processes include semiconductors such as microprocessors, memory chips and application specific integrated circuits (ASICs), printed circuit boards, power supplies and enclosures.

Our external manufacturing operations consists primarily of hardware assembly and configuration and the loading of the appropriate software.

Intellectual Property and Licenses

Our success and our ability to compete are dependent, in part, upon our proprietary technology. While we have applied for certain patents, we currently rely on a combination of contractual rights, trade secrets and copyright laws to establish and protect our proprietary rights in our products. We have also entered into non-disclosure agreements with our suppliers, resellers and certain customers to limit access to and disclosure of proprietary information. There can be no assurance that the steps taken by us to protect our intellectual property will be adequate to prevent misappropriation of our technology or that our competitors will not independently develop technologies that are substantially equivalent or superior to our technology.

We have entered into software and product license agreements with various suppliers. These license agreements provide us with additional software and hardware components that add value to our security products. These license agreements do not provide proprietary rights that are unique or exclusive to us and are generally available to other parties on the same or similar terms and conditions, subject to payment of applicable license fees and royalties.

Sales, Marketing and Customers

Field Sales Force. Our direct sales organization focuses on major account sales, channel partners including distributors, Value Added Resellers (VARs) and integrators; promotes our products to current and potential customers; and monitors evolving customer requirements. The field sales and technical support force provides training and technical support to our resellers and end users and assists our customers to design secure data networking solutions.

We currently conduct sales and marketing efforts from our principal office in Richardson (Dallas), Texas and through foreign sales offices located in the following countries: England, France and Malaysia. In addition, we have sales personnel, sales engineers or sales representatives located in Los Angeles, Eastern Europe and Spain.

Distributors. We have signed distribution agreements with distributors in the United States, Europe and Asia. In general, these relationships are non-exclusive. Distributors typically maintain an inventory of our products. Under these agreements, we provide certain protection to the distributors for their inventory of our products for price reductions as well as products that are slow moving or have been discontinued. Recognition of sales to distributors and related gross profits are deferred until the distributors resell the merchandise. However, since we have legally sold the inventory to the distributor and we no longer have care, custody or control over the inventory, we recognize the trade accounts receivable and reduce inventory related to the sale at the time of shipment to the distributor.

Resellers. Domestic and international system integrators and VARs (collectively, resellers) sell our products as stand-alone solutions to end users and integrate our products with products sold by other vendors into network security systems that are sold to end users. Our field sales force and technical support organization provide support to these resellers. Our agreements with resellers are non-exclusive, and our resellers generally sell other products that may compete with our products. Resellers may place higher priority on products of other suppliers who are larger than and have more name recognition than us, and there can be no assurance that resellers will continue to sell and support our products.

Foreign Sales. We believe that rapidly evolving international markets are important sources of future net sales. Our export sales are currently being made through a direct sales force supplemented by international resellers in Europe, Asia and Canada. Export sales accounted for approximately 31.4%, 33.4% and 36.4% of net sales in 2003, 2002 and 2001, respectively. See Management s Discussion and Analysis of Financial Condition and Results of Operations included in this report for a geographic breakdown of our product revenue in 2003, 2002 and 2001. Sales to foreign customers and resellers generally have been made in United States dollars.

Marketing. We have implemented several methods to market our products, including public relations and placed articles, regular participation in and presenting during trade shows and seminars, advertisement in trade journals, telemarketing, distribution of sales literature and product specifications and ongoing communication with our resellers and installed base of end-user customers.

Customers. Our end-user customers include manufacturing, high technology, telecommunications, retail, transportation, health care, insurance, entertainment, utilities and energy companies, government agencies, financial institutions and academic institutions. Sales to certain customers and groups of customers can be impacted by seasonal capital expenditure approval cycles, and sales to customers within certain geographic regions can be subject to seasonal fluctuations in demand.

Although we sell our products to many customers, through various distribution channels, no one customer or reseller accounted for 10% or more of our net sales in any of the past three fiscal years.

However, in 2003, 17.0% of our revenue was derived from the sales to a variety of U.S. government entities through system integrators and resellers. The loss of sales to the various U.S. government agencies could have a material adverse effect on our business and operating results if not replaced. No other customer accounted for 10% or more of our net sales in 2003, 2002 or 2001, respectively.

Backlog. We believe that only a small portion of our order backlog is non-cancelable and that the dollar amount associated with the non-cancelable portion is immaterial. We purchase inventory based upon our forecast of customer demand and maintain inventories of sub-assemblies and finished products in advance of receiving firm orders from customers. Orders are generally fulfilled within two days to two weeks following receipt of an order. Due to the generally short cycle between order and shipment and occasional customer-initiated changes in delivery schedules or cancellation of orders that are made without significant penalty, we do not believe that our backlog as of any particular date is indicative of future net sales.

Customer Support, Service and Warranty. We service, repair and provide technical support for our products. Our field sales and technical support force works closely with resellers and end-user customers on-site and by telephone to assist with pre- and post-sales support services such as network security design, system installation and technical consulting. By working closely with our customers, our employees increase their understanding of end-user requirements and provide

input to the product development process.

We warrant all of our products against defects in materials and workmanship for periods ranging from 90 days to 12 months. Before and after expiration of the product warranty period, we offer both on-site and factory-based support, parts replacement and repair services. Extended warranty services are separately invoiced on a time and materials basis or under an annual maintenance contract.

Competition

The market for network security solutions is intensely competitive and subject to frequent product introductions with new technologies, improved price and performance characteristics. Industry suppliers compete in areas such as conformity to existing and emerging industry standards, interoperability with networking and other security products, management and security capabilities, performance, price, ease of use, scalability, reliability, flexibility, product features and technical support. We believe that our approach focusing on the network perimeters with market leading network intrusion detection technology that reduces the total cost of ownership compared to the competition provides us with an advantage with large organizations with complex security requirements.

There are numerous companies competing in various segments of the data security markets. Our principle competitors in the network intrusion prevention and detection market include Internet Security Systems, Inc., Cisco Systems, Inc., Symantec, Inc., Netscreen Technologies, Inc., Network Associates, Inc., Tipping Point Technologies Inc., and NFR Security, Inc. Our competitors in the regulated information compliance market include a small number of start up companies that entered the space within the last two-years. Several of our competitors have substantially greater financial, technical, sales and marketing resources, better name recognition and a larger customer base than we do. In addition, many of our competitors may provide a more comprehensive networking and security solution than we currently offer. Even if we do introduce advanced products, which meet evolving customer requirements in a timely manner, there can be no assurance that our new products will gain market acceptance.

Certain companies in the network security industry have expanded their product lines or technologies in recent years as a result of acquisitions. Further, more companies have developed products which conform to existing and emerging industry standards and have sought to compete on the basis of price. We anticipate increased competition from large networking equipment vendors, which are expanding their capabilities in the network security market. In addition, we anticipate increased competition from private start-up companies that have developed or are developing advanced security products. Increased competition in the security industry could result in significant price competition, reduced profit margins or loss of market share, any of which could have a material adverse effect on our business, operating results and financial condition. There can be no assurance that we will be able to compete successfully in the future with current or new competitors.

Employees

As of December 31, 2003, we employed a total of 44 persons, including 17 in sales, marketing and technical support, 3 in manufacturing and operations, 15 in research and product development and 9 in administration and finance.

None of our employees are represented by a labor organization, and we are not a party to any collective bargaining agreement. We have not experienced any work stoppages and consider our relations with our employees to be good.

Competition in the recruiting of personnel in the networking and data security industry is intense. We believe that our future success will depend in part on our continued ability to hire, motivate and retain qualified management, sales and marketing, and technical personnel. To date, we have not experienced significant difficulties in attracting or retaining qualified employees.

Factors That May Affect Future Results of Operations

In addition to the other information in this Form 10-K, the following factors should be considered in evaluating Intrusion Inc. and our business. This report may include various non-GAAP financial measures (as defined by SEC Regulation G), including our cash used in operations excluding costs associated with a litigation settlement and severance charges. Our management believes these measures provide useful information to investors about our financial condition and results of operations for the period presented by eliminating the affects of one-time and other transactions that can distort underlying operational results in order to provide greater comparability of our financial performance on a year-to-year basis. The most directly comparable GAAP financial measures and reconciliation of the difference between GAAP and non-GAAP financial measures can be found in the test of this report and our consolidated financial statements included in this report.

10

Sufficiency of Cash Flow. As of December 31, 2003, we had cash, cash equivalents and investments in the amount of approximately $2.7 million, down from approximately $10.7 million as of December 31, 2002. However, throughout 2003, we reduced expenses. As a result, our cash used in operations, net of the litigation settlement and severance charges, for the fourth quarter was approximately $1.4 million. Including litigation settlement and severance charges, our cash used in operation in the fourth quarter of 2003 was $1.9 million. On March 25, 2004, we closed a $5.0 million private placement of 5% Convertible Preferred Stock and warrants. With this additional financing, we believe that we have sufficient cash resources to finance our operations and expected capital expenditures for the next twelve months. The sufficiency of our cash resources may depend to a certain extent on general economic, financial, competitive or other factors beyond our control. Moreover, despite actions to reduce our cost and improve our profitability, we expect our operating losses and net operating cash outflows to continue through at least the first half of 2004. We do not currently have any further arrangements for financing, and we may not be able to secure additional debt or equity financing on terms that are acceptable to us, or at all, at the time when we need such funding. If our business does not generate sufficient cash flow from operations and sufficient financings are not available, we may not be able to operate or grow our business, pay our expenses when due or fund our other liquidity needs.

Technological Changes. The market for our products is characterized by frequent product introductions, rapidly changing technology and continued evolution of new industry standards. The market for security products requires our products to be compatible and interoperable with products and architectures offered by various vendors, including other security products, networking products, workstation and personal computer architectures and computer and network operating systems. Our success will depend to a substantial degree upon our ability to develop and introduce in a timely manner new products and enhancements to our existing products that meet changing customer requirements and evolving industry standards. The development of technologically advanced products is a complex and uncertain process requiring high levels of innovation as well as the accurate anticipation of technological and market trends. There can be no assurance that we will be able to identify, develop, manufacture, market and support new or enhanced products successfully in a timely manner. Further, we or our competitors may introduce new products or product enhancements that shorten the life cycle of or obsolete our existing product lines, any of which could have a material adverse effect on our business, operating results and financial condition.

Market Acceptance. We are pursuing a strategy to increase the percentage of our revenue generated through indirect sales channels including distributors, VARs, system integrators, original equipment manufacturers and managed service providers. There can be no assurance that our products will gain market acceptance in these indirect sales channels. Further, competition among security companies to sell products through these indirect sales channels could result in significant price competition and reduced profit margins.

We are also pursuing a strategy to further differentiate our product line by introducing complementary security products and incorporating new technologies into our existing product line. There can be no assurance that we will successfully introduce these products or that such products will gain market acceptance. We anticipate competition from networking companies, network security companies and others in each of our product lines. We anticipate that profit margins will vary among our product lines and that product mix fluctuations could have an adverse effect on our overall profit margins.

Acquisitions. Some of our competitors have acquired several security companies with complementary technologies, and we anticipate that such acquisitions will continue in the future. These acquisitions may permit such competitors to accelerate the development and commercialization of broader product lines and more comprehensive solutions than we currently offer. In the past, we have relied upon a combination of internal product development and partnerships with other security vendors to provide competitive solutions to customers. Certain of the recent and future acquisitions by our competitors may have the effect of limiting our access to commercially significant technologies. Further, the business combinations and acquisitions in the security industry are creating companies with larger market shares, customer bases, sales forces, product offerings and technology and marketing expertise. There can be no assurance that we will be able to compete successfully in such an environment.

We have made acquisitions in the past, and we may, in the future, acquire or invest in additional companies, business units, product lines, or technologies to accelerate the development of products and sales channels complementary to our existing products and sales channels. Acquisitions involve numerous risks, including: difficulties in assimilation of operations, technologies, and products of the acquired companies; risks of entering markets in which we have no or limited direct prior experience and where competitors in such markets have stronger market positions; the potential loss of key employees of the acquired company; and the diversion of our attention from normal daily operation of our business. There can be no assurance that any other acquisition or investment will be consummated or that such acquisition or investment will be realized.

Product Transitions. Once current security products have been in the market place for a period of time and begin to be replaced by higher performance products (whether of our design or a competitor s design), we expect the net sales of such products to decrease. In order to achieve revenue growth in the future, we will be required to design, develop and successfully commercialize higher performance products in a timely manner. There can be no assurance that we will be able to introduce new products and gain market acceptance quickly enough to avoid adverse revenue transition patterns during current or future product transitions. Nor can there be any assurance that we will be able to respond effectively to technological changes or new product announcements by competitors, which could render portions of our inventory obsolete.

Manufacturing and Suppliers. Our operational strategy relies on outsourcing of product assembly and certain other operations. There can be no assurance that we will effectively manage our third-party contractors or that these contractors will meet our future requirements for timely delivery of products of sufficient quality and quantity. Further, we intend to introduce a number of new products and product enhancements in 2004 that will require that we rapidly achieve volume production of those new products by coordinating our efforts with those of our suppliers and contractors. The inability of the third-party contractors to provide us with adequate supplies of high-quality products could cause a delay in our ability to fulfill orders and could have an adverse effect on our business, operating results and financial condition.

All of the materials used in our products are purchased under contracts or purchase orders with third parties. While we believe that many of the materials used in the production of our products are generally readily available from a variety of sources, certain components such as microprocessors and motherboards are available from one or a limited number of suppliers. The lead times for delivery of components vary significantly and can exceed twelve weeks for certain components. If we should fail to forecast our requirements accurately for components, we may experience excess inventory or shortages of certain components that could have an adverse effect on our business and operating results. Further, any interruption in the supply of any of these components, or the inability to procure these components from alternative sources at acceptable prices within a reasonable time, could have an adverse effect on our business and operating results.

Intellectual Property and Licenses. There are many patents held by companies, which relate to the design and manufacture of network security systems. The holders of those patents could assert potential claims of infringement. We could incur substantial costs in defending our company and our customers against any such claim regardless of the merits of such claims. In the event of a successful claim of infringement, we may be required to obtain one or more licenses from third parties. There can be no assurance that we could obtain the necessary licenses on reasonable terms.

Dependence on Check Point Technologies. Our PDS family of security appliances, which are integrated with Check Point Software Technologies VPN-1®/FireWall-1® software, represents 16.7% of our 2003 sales, which is down from 29.1% of our sales in 2002. We expect that the percentage of PDS family sales will continue to decrease as we move away from the Check Point Software Technologies solutions. Our long-term plans are for a continued decline in revenue from the PDS family of products. Our reliance on newer product sales may not replace the anticipated decline in revenue of the PDS family product sales. Although we are a certified appliance partner of Check Point and our PDS products have received certification from Check Point, we have no long-term agreement or exclusive relationship with Check Point. As a result, the loss or significant change in our relationship with Check Point, the failure of future PDS products to receive Check Point certification, the business failure of Check Point or its acquisition by or of one of our competitors, and the loss of market share of Check Point or market acceptance of its products could each have a material adverse effect on our business, financial condition and results of operations.

Third-Party Products. We believe that it is beneficial to work with third parties with complementary technologies to broaden the appeal of our security products. These alliances allow us to provide integrated solutions to our customers by combining our developed technology with third-party products. As there is rapid technological advancement and significant consolidation in the network security industry, there can be no assurance that we will have access to all of the third-party products that may be desirable or for the term desirable to offer fully integrated solutions to our customers.

Dependence on Key Customers. In the past, a relatively small number of customers have accounted for a significant portion of our revenue. Although no single customer currently accounts for more than 10% of our revenue, we expect to continue to derive a substantial portion of our net revenue from sales to U.S. government agencies, large system integrators and managed service providers. We continuously face competition from Internet Security Systems, Cisco, Enterasys, NFR, IBM, Hewlett Packard and others for U.S. government security projects and corporate security installations. Any reduction or delay in sales of our products to these customers could have a material adverse effect on our operating results.

International Operations. Foreign sales accounted for approximately 31.4% of our revenue in 2003, and we expect sales to foreign customers to continue to represent a significant portion of our revenues in the future. Our international operations may be affected by changes in demand resulting from fluctuations in currency exchange rates and local purchasing practices, including seasonal fluctuations in demand, as well as by risks such as increases in duty rates, difficulties in distribution, regulatory approvals and other constraints upon international trade. Our sales to foreign customers are subject to export regulations. In particular, certain sales of our data security products require clearance and export licenses from the U.S. Department of Commerce under these regulations. Any inability to obtain such clearances or any required foreign regulatory approvals on a timely basis could have a material adverse effect on our operating results.

Impact of Government Customers. For the fiscal year ended December 31 2003, 17.0% of our revenue was derived from sales to various U.S. government entities, either directly by us or through system integrators and other resellers, compared to 20% for the fiscal year ended December 31, 2002, and 2.6% of our revenue for 2003 was derived from sales to foreign government entities as compared to 0.4% for 2002. Sales to the government present risks in addition to those involved in sales to commercial customers, including potential disruption due to appropriation and spending patterns and the government s reservation of the right to cancel contracts and purchase order for its convenience.

Effects of Military Actions. United States military actions or other events occurring in response or in connection to them, including future terrorist attacks against United States targets, actual conflicts involving the United States or its allies or military or trade disruptions could impact our operations, including by:

Reducing government or corporate spending on network security products;

Increasing the cost and difficulty in obtaining materials or shipping products; and

Affecting our ability to conduct business internationally.

Should such events occur, our business, operating results and financial condition could be materially and adversely affected.

Restructuring and Cost Reductions. We continued with our restructuring plan in 2003, which resulted in $0.5 million in severance charges. The objective of our restructuring plan was to reduce our cost structure to a sustainable level that is consistent with the current macroeconomic environment. We also implemented other strategic initiatives designed to strengthen our operations. These plans involved, among other things, reductions in our workforce and facilities, aligning our organization around our business objectives, realignment of our research and development team, our sales force and changes in our sales management. Any further workforce reductions could result in temporary reduced productivity of our remaining employees. Additionally, our customers and prospects may delay or forgo purchasing our products due to a perceived uncertainty caused by the restructuring and other changes. Failure to achieve the desired results of our initiatives could seriously harm our business, results of operations and financial condition.

Potential Nasdaq Delisting. On August 12, 2002, Nasdaq notified the Company that the Company s Common Stock had not maintained the required minimum bid price per share for continued inclusion on The Nasdaq National Market and was granted a 90-day extension until November 11, 2002 to regain compliance. The Company failed to remedy the deficiency and, on November 4, 2002, filed an application to transfer the listing of its Common Stock from The Nasdaq National Market to The Nasdaq SmallCap Market. The Company s Common Stock began trading on The Nasdaq SmallCap Market on December 4, 2002. In accordance with Nasdaq rules, the Company was granted the remainder of a 180-day grace period afforded to Nasdaq SmallCap issuers, which expired on February 10, 2003. At that time, the Company was granted an additional 180-day grace period to remedy the bid price deficiency which expired on August 7, 2003, after which, Nasdaq granted the Company a final 90-day extension through November 5, 2003 to regain compliance. On November 6, 2003, the Company received a delisting notice from Nasdaq stating that the Company s Common Stock would be delisted at the close of business on November 17, 2003 because the Company had not regained compliance with the minimum $1.00 bid price per share requirement.