# NSA Technology Transfer Program

ACCESS TO INNOVATION

TTP

National Security Agency, 9800 Savage Road, Suite 6541, Ft. Meade, MD 20755-6541

## WELCOME

The National Security Agency/Central Security Service (NSA/CSS) drives one of the U.S. government's leading research and development (R&D) programs.

NSA scientists and engineers, along with our academic and research partners, develop cutting-edge technologies to meet agency mission requirements.

Our discoveries also contribute to the creation and improvement of many commercial products.

Through our Technology Transfer Program, NSA openly shares these technologies with private industry, academia, and U.S. government agencies.

# NSA Technology Transfer Program

National Security Agency, 9800 Savage Road, Suite 6541, Ft. Meade, MD 20755-6541

# Table of Contents

NSA is America's cryptologic organization. It coordinates, directs, and performs highly specialized activities to protect U.S. government information systems and produce foreign signals intelligence information. NSA is on the forefront of communications and data processing. It is also one of the most important centers of foreign language analysis and research within the U.S. government.

NSA's early interest in cryptanalytic research led to the first large-scale computer and the first solid-state computer, predecessors to the modern computer. NSA pioneered efforts in flexible storage capabilities, which led to the development of the tape cassette. NSA also made groundbreaking developments in semiconductor technology and remains a world leader in many technological fields.

NSA headquarters is located at Ft. Meade, Maryland. Its workforce represents an unusual combination of specialties: analysts, engineers, physicists, mathematicians, linguists, computer scientists, and researchers.

NSA recognizes the value of its investments in R&D activities and the potential impact of these activities for enhancing the U.S. economy. More importantly, NSA appreciates that leveraging its R&D with others can have a significant impact on its ability to meet the dynamic, time sensitive requirements of its mission. This recognition is why the Agency actively participates, supports, and encourages technology transfer through its Technology Transfer Program (TTP).

The NSA TTP provides commercial, academic, and government entities access to NSA-developed technologies and collaborative R&D opportunities. These technologies and capabilities can result in significant cost savings, technological advancements, and profits for those organizations that leverage this resource.

NSA's TTP officially launched in 1990 under the legislative authority of the Technology Transfer Act of 1986. Since its inception, the program has provided a venue for NSA employees to share federally-funded research and to conduct collaborative research with academia, private industry, other federal agencies, and state and local governments.

The TTP Office facilitates the exploration and formalization of partnerships between NSA and outside organizations to achieve specific objectives.

The primary objective of NSA's TTP Office is to transfer NSA-developed technology to commercial enterprises to strengthen the U.S. industrial base and accept commercial-off-the-shelf (COTS) technology for government use to reduce the cost of items purchased by the federal government by:

- Developing dual-use technologies for application by the government and the commercial marketplace
- Accelerating development of emerging technologies
- Leveraging external subject-matter expertise and resources to address government and industry needs

NSA is proactively seeking partnerships with government, academic, and industrial organizations that will work with the Agency to meet NSA mission objectives through the TTP. Licensing, collaborative R&D, education partnerships, and other opportunities are available within these key areas:

- Communications and Networking
- Advanced Mathematics
- Advanced Computing
- Information Processing
- Microelectronics

Through a series of well-defined processes and procedures, TTP and NSA's Office of General Counsel (OGC) draft, facilitate, negotiate, and broker each TTP agreement.

To explore opportunities available through the NSA Technology Transfer Program, please visit our website:

http://www.nsa.gov/research/tech_transfer

Call 443-445-7159, or write to:

NSA Technology Transfer Program
9800 Savage Road, Suite 6541
Ft. Meade, MD 20755-6541

## What is Technology Transfer?

In the context of federal laboratories, it is the sharing of information, intellectual property (IP), expertise, and technology between the laboratories and non-federal entities (i.e., state and local governments, universities, non-profit organizations, and private industry). It consists of transfers at various levels within the technology lifecycle, ranging from conception to the actual selling of products or services in the marketplace.

TTP primarily facilitates Patent License Agreements, Cooperative Research and Development Agreements, Education Partnership Agreements, and Technology Transfer Sharing Agreements.

## Benefits of Technology Transfer

Technology transfer offers benefits for both the government and non-federal entities. The most prominent benefits for engaging in technology transfer activities include:

- Using outside technical expertise and resources to help accomplish NSA's mission-oriented activities through collaborative efforts between the government and a non-federal entity
- Leveraging federally-funded R&D to create new applications and commercial products or services
- Using government R&D investment to support commercial needs and create a positive impact on U.S. economy
- Using government facilities to conduct R&D efforts rather than building new facilities
- Obtaining financial gains for the government and employees from royalty payments for those technology transfers that involve patent licenses
- Creating an opportunity for university researchers and students to gain valuable learning experience from collaboration with leading NSA scientists, researchers, and developers.

## Types of Technology Transfer

The technology transfer process is dependent on the type and goal of the transfer. The main types of transfer include:

- Commercial Transfer - Transfer of federally-owned technologies to the private sector to develop new or improved technologies, materials, processes, products, or services which are made available to the public
- Exporting Resources - Federal personnel provide expertise, IP, equipment, and consultation to non-federal entities
- Importing Resources - Federal personnel engage with non-federal entities to bring outside technology into the agency to enhance mission-oriented efforts
- Dual Use - Federal laboratories partner with industry to jointly develop dual-use technologies, which has a direct benefit to the warfighter's mission as well as to the industrial partner's competitive position in the marketplace

There are many laws that promote technology transfer and provide technology transfer mechanisms and incentives. The following are highlights of some of the federal legislation that apply to NSA's TTP Program.

## Stevenson-Wydler Technology Innovation Act of 1980 (P.L. 96-480)

defines technology transfer and encourages federal laboratories to engage in cooperative research with state and local governments, academia, nonprofit organizations, or private industry. Its provisions also established and defined the basic activities of an Office of Research and Technology Applications (ORTA) at each federal laboratory, and set aside a small percentage of each laboratory's budget to fund technology transfer activities.

## Bayh-Dole Act of 1980 (P.L.96-517)

permits universities, small businesses, and nonprofit organizations to obtain title to inventions developed with federal funds. This policy also allows the federal agency to retain an irrevocable license to use the invention. This policy permits federal laboratories to grant exclusive patent licenses to industry.

## 15 United States Code, Section 3710a

when entering into a CRADA agreement, preference shall be given to business units located in the U.S. which agree to substantially manufacture products in the U.S.

## Federal Technology Transfer Act of 1986 (P.L.99-502)

requires scientists and engineers to consider technology transfer an individual responsibility. It also enables federal labs to negotiate licensing arrangements for patented inventions and requires that federal inventors share in royalties from patent licenses. It establishes a charter and funding mechanism for the Federal Laboratory Consortium (FLC). The FLC is responsible for a variety of activities including providing training courses and assistance for technology transfer programs.

## Executive Order 12591 of 1987

ensures that federal labs assist universities and the private sector by transferring technical knowledge. It also promotes commercialization of federally-funded inventions by requiring that laboratories grant contractors the title to patents developed with federal funds, as long as the government is given a royalty-free license for use.

Organizationally located in NSA's Research Directorate, TTP provides services to all NSA organizations and individuals who desire to participate in technology transfer activities. TTP offers services in the areas of Opportunity Management, Customer Service, Intellectual Asset Management, Program and Technology Marketing, and Rewards and Recognition.

The process is initiated when a client contacts the TTP customer service center. Initial contact and company information is captured by the call center, and companies interested in engaging in technology transfer with NSA are required to sign a Non-Disclosure Agreement.

Each client is assigned to a Technology Transfer Agent who will work with the company and the relevant NSA organizations to facilitate and ratify all appropriate technology transfer agreements.

## Opportunity Management (OM)

OM addresses technology transfer inquiries from industry, academia, or government employees. OM identifies the appropriate agreement for the technology transfer and includes the facilitation and negotiation of the TTP agreement.

TTP agreements include: Cooperative Research and Development Agreements (CRADAs), Patent License Agreements (PLAs), Education and Industry Partnership Agreements (EPA/IPAs), and Technology Transfer Sharing Agreements (TTSAs).

The major activities involved in the OM process are:

- Requirement Assessment
- Transfer Vehicle Identification
- Strategy Development
- Proposals and Negotiations
- Transfer Vehicle Execution
- Transfer Vehicle Management

## Customer Service

TTP has a Customer Service Center to support and act as a focal point for both outside and Agency-sponsored technology transfer opportunities. A well-defined procedure has been established to track and respond to TTP inquiries.

## Intellectual Asset Management (IAM)

IAM focuses on maximizing the value of NSA's IP through the collective processes of identification, collection, assessment, management, and protection.

The IAM process is initiated when a researcher, technologist, or developer submits an invention disclosure package to the OGC. Once the OGC determines ownership and whether IP protection is appropriate, a copy of the invention disclosure package is reviewed by the Technology Transfer Assessment Panel (TTAP). The TTAP is an internal panel comprised of senior technical directors, who review the invention disclosure package for suitability for public release and whether patent protection should be pursued.

If the TTAP approves the invention disclosure as a patent candidate for public release, the NSA patent attorneys write and file a patent application with the United States Patent and Trademark Office. Simultaneously, TTP adds the technology to its Intellectual Assets Portfolio and it becomes a candidate for a patent license agreement. If TTAP decides that the invention is not suitable for patent prosecution or public release, then the IAM lifecycle for that particular invention is complete.

Once a technology becomes part of the Intellectual Asset Portfolio, TTP may conduct the following activities:

- Interview inventors/technologists to obtain technical support
- Conduct technology evaluations to determine commercial potential and benefits
- Conduct/obtain market assessments and valuations to determine potential industry areas and an approximate value of the technology to these markets
- Create Technology Profile Fact Sheets for posting on the nsa.gov website
- Track transfers to other organizations
- Monitor and track any patent-related fees

## Program and Technology Marketing

Program marketing includes activities that support internal and external promotion of the TTP, its services, and capabilities. The goals of the promotional activities are to:

- Encourage NSA employees to participate in technology transfer activities
- Promote the benefits of the program to internal and external organizations
- Identify potential partners based upon mission and industry needs
- Identify commercialization opportunities

Technology marketing is geared to promoting specific technologies at industry-sponsored events. The goal of this marketing is to identify potential licensees within specific markets for which the commercialization of these technologies would benefit the most.

TTP conducts program awareness and technology-focused marketing through a variety of promotion techniques:

- Publication of Technology Profile Fact Sheets on the nsa.gov website
- NSA publications
- Presentations to external and internal organizations
- Attendance at academic, government, trade shows, and exhibitions

## Rewards and Recognition

Technology transfer legislation allows for the reward and recognition of those employees who participate in technology transfer activities or substantially increase the value of the inventions. These individuals share in a percentage of license fees and royalty payments, which can result from the licensing of a patent.

TTP is responsible for handling, monitoring, tracking, and distributing all royalty payments and fees. To recognize participation in the technology transfer process, NSA distributes $2000 for the award of the patent, plus more than the minimum 15% legislative requirement of collected royalties to its government researchers.

## Patent License Agreements (PLA)

Title 35 U.S.C. 207-209 gives NSA the authority to grant licenses on its domestic and foreign patents and patent applications. This authority is implemented through PLAs. The goal of these licenses is to provide the private sector the opportunity to commercially develop federally-funded research to promote economic growth and global competitiveness.

## PLA Benefits

- Encourages commercialization of federally-funded research in the private sector
- Saves industry and academia the cost and time of conducting R&D
- Provides royalty income to the government and its inventors
- Creates new industry and employment opportunities in the private sector
- Maximizes the value of NSA's R&D investment and resulting technologies

## Licensing Policy

A license may be non-exclusive, partially exclusive, or exclusive. The licensee must complete a Letter of Application and submit for evaluation a Business Plan that outlines the licensee's approach to commercialization and marketing of the invention. In general, a licensee must agree to substantially manufacture products in the U.S.

The licensee must make the invention available to the public within a specified period of time and continue to make the benefits of the invention reasonably accessible to the public. The licensee must agree to report periodically on the use of the patent to NSA.

All NSA license agreements are individually negotiated with the prospective licensees on terms concerning license durations, reporting periods, fees, and royalty payments. The government always retains irrevocable, royalty free, worldwide government purpose rights to the invention.

NSA retains the right to terminate patent license agreements if the prospective licensee is unable to execute their business plan or achieve practical application as negotiated between prospective licensee and inventor/technologists.

## Cooperative Research and Development Agreement - CRADA

The CRADA is one of the most valuable technology transfer mechanisms for obtaining long-term value. Title 15 U.S.C. 3710 gives NSA the authority to enter into CRADAs to foster collaborative relationships with industry, local and state governments, and academia to obtain valuable technology transfer goals and benefits.

## CRADA Benefits

- Creates new products, processes, and intellectual property applicable to mission and/or commercial goals
- Modifies commercial products for government use in mission applications
- Reduces cost and time of R&D to achieve mission and/or commercial goals
- Leverages external expertise, ideas, investment and resources
- Provides a joint approach to solving specific problems by applying different cultural solutions
- Increases probability to commercialize inventions made under a CRADA
- Increases awareness of market and technology trends and the needs of industry and government

## CRADA Elements

- Legal and business framework for the management and execution of the CRADA
- Statement of Work (SOW) that sets forth the nature and scope of research and development to be conducted
- Estimation of resources that will be used in the performance of the CRADA
- Reports for CRADA status and IP discovery
- Financial obligations that specify the amount of funds a partner will pay, if applicable
- Contact information for management and technical issues
- Ownership of inventions and copyrights brought into the CRADA and created from joint research performed under the CRADA
- Rights and protections given to proprietary information brought into the CRADA and developed under the CRADA

## Education Partnership Agreement (EPA)

The purpose of an Education Partnership Agreement is to formalize the relationship between a federal lab and an educational institution. Title 10 U.S.C. 2194 allows NSA to share its unique experience by providing training to personnel in the science and technology fields at all education levels using EPAs.

## EPA Benefits

- Involving students to ensure a future resource of scientists, mathematicians, and engineers
- Providing unique opportunities for learning not available from other resources
- Providing access to laboratory personnel available to teach courses and develop science curriculums
- Permitting students and teachers to become involved in developing useful technological applications
- Providing access to NSA resources, either through excess status or loan, which relieves institutions from some of the financial burden of R&D investment

## EPA Elements

IP rights to inventions created under the agreement:

- Protections given to proprietary information brought into an agreement and developed under the agreement
- Task Plan outlining the learning objectives and goals
- List of equipment to be loaned, if applicable

# Technology Transfer MECHANISMS

## Technology Transfer Sharing Agreement (TTSA)

TTSAs protect NSA's right to seek commercialization of technologies it owns, and to effectively track the transfer of these technologies.

## TTSA Benefits

- Simple agreements that specify the purpose, terms, and conditions related to the transfer
- Allows for easy transition of technology between U.S. government agencies

## TTSA Elements

TTSAs include specific language regarding non-commercialization and restrict the transfer for government use only.

TTP only accepts TTSA requests from NSA government personnel. Contractors and other partners requiring technology in support of a contract must have their government Contractor Officer Representative (COR) or Program Manager submit the request to TTP on their behalf. Government organizations may submit their request directly to TTP.

NSA has identified valuable advanced technologies in the following core areas, which are available for sharing:

COMMUNICATIONS AND NETWORKING
ADVANCED MATHEMATICS
ADVANCED COMPUTING
INFORMATION PROCESSING
MICROELECTRONICS

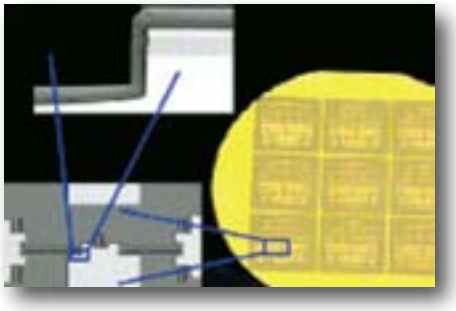
The core technologies presented in this booklet represent a small subset of NSA technologies available for licensing. A complete listing of NSA Technology Profile Fact Sheets can be found on www.nsa.gov/research/tech_transfer

*As our advancements in communication and networking techniques continue, they will provide new opportunities to deliver vast amounts of data more efficiently and reliably.*

NSA is a demanding consumer and an aggressive developer of communications and networking equipment and products. Expanding capabilities currently include advancements in packet and switching technology, more sophisticated network structures, improved multimedia communications networks, ultra-high data rates, new compression techniques plus progressive mobile and satellite communication services.

The growing need to selectively distribute different levels of information over common networks has led to the Multilevel Information Systems Security Initiative (MISSI) and an evolving family of products. Additionally, the federal government now uses the STU-III telephone developed by the NSA for secure voice communications.

As NSA's advancements in communications and networking techniques continue, they will provide new opportunities to deliver vast amounts of data more efficiently and reliably. In turn, technology users will continue to benefit from technical assistance and move toward resolving interoperability issues.



## *Photonic Logic Device Suite*

*Electronic components may dominate today's $100 billion semiconductor market, but a new technology is emerging that could make them obsolete. Integrated Photonics already promise to deliver what traditional electronics can't — bandwidth and speed.*

Electronic semiconductors are not keeping pace with the demands for speed and bandwidth that multimedia applications, like Video-on-Demand and Broadband TV, require. The creation of fully photonic components is needed to replace traditional electronic devices.

NSA's Photonic Logic Device Suite lays the groundwork for the commercial development of an integrated photonics device. This suite of eight inventions overcomes the drawbacks and inefficiencies of previous methods, decreasing manufacturing costs, and improving the efficiency of integrated photonic devices.

*Mode Transition-Discrimination Photonic Logic Device:* An optical device for the implementation of invert or XOR logic. It is designed to be compact, to allow accurate discrimination between modes of the output signal, and to accept an input signal off-axis with respect to the output signal, preventing unintended signal scattering back into the input waveguides.

*Method of Determining Semiconductor-Laser Facet Reflectivity After Reflectance Modification:* Method for measuring the amount of light a laser facet (mirror) reflects back into a laser after the facet reflectance has been modified. Employs measurement tools already required for fabrication of semiconductor lasers, also works on lasers with coated or uncoated facets. Method to measure gain of a side-injection input photonic inverter, based on a semiconductor laser using two different modes of operation.

*Method for Measuring Gain of Photonic Inverters:* In one mode, the device operates as a photonic inverter; in the other, as a photo generated current measurement device. Captures an essential manufacturing metric. Overcomes the measuring errors currently associated with photonic inverters, including errors introduced by insertion loss.

*Method of Coating Multiple Optical Device Facets with Dielectric Layers:* Method of depositing layers of dielectric on facets of an optical semiconductor device (such as a ridge laser) for the purpose of controlling reflectance. Allows for quick modification of reflectance of facets using PECVD or a like method.

*Photonic Logic Device Fabrication Using Sacrificial Spacer Layers:* These four inventions describe methods of constructing air gaps, waveguides, shadow masks, and mirrors on an optical semiconductor device by depositing spacer layers and then removing ('sacrificing') them.

*Method of Fabricating Waveguide using Sacrificial Spacer Layer:* Controlled coupling of a semiconductor laser into the waveguide.

*Method of Fabricating Turning Mirror Using a Sacrificial Spacer Layer:* For optical routing of integrated optical signals.

*Method of Fabricating a Patterned Device Using a Sacrificial Spacer Layer:* Avoids time-consuming, costly, high-resolution deep-UV or electron-beam lithographic steps for sub-micron shadow mask fabrication. Enables precise line width control of patterned optoelectronic and microelectronic devices.

*Method of Fabricating Optical Device Using Multiple Sacrificial Spacer Layers:* Increased spectral width and large range of reflectance in multiple air gap mirror structures.


## *Detecting and Controlling Malicious Software*

*Computer worms and viruses are more than an inconvenience to computer users worldwide. They pose a threat to national security and result in millions of dollars in recovery costs each year.*

These self-replicating programs exploit vulnerabilities in the targeted computer or network, resulting in system crashes, denial of service, and the corruption or destruction of critical and sensitive information. Now that most personal computers are connected to the internet and to local area networks, the spread of malicious codes and software is even more of a threat to computer users at all levels: from home users to medical, financial, government, and industrial users, among others.

NSA researchers recognize the severity of this problem and have developed a new technology that can severely limit the spread of both computer viruses and worms. This new technology is able to block or identify when an untrusted code tries to exploit a programming flaw on the targeted system. NSA's detection process identifies or blocks this network-run software, distinguishing it from software stored locally on the targeted system. This exciting new methodology works in combination with other anti-virus products and can also serve as the basis of a new and powerful tool for identifying software delivered over a computer network and the mechanism for governing its execution.


## *NetTop®*

*Both the private and public sectors face challenges to improve the operational efficiency of their IT systems while reducing costs, and maintaining a high level of information security. NetTop® addresses these challenges by reducing the need for multiple workstations, allowing access to applications previously isolated on separate networks, and providing a high level of security.*

Researchers at NSA's National Information Assurance Research Laboratory have invented and developed a modular architecture predominately based on COTS, which removes security functionality from the control of the end-user operating system and applications.

NetTop® incorporates typical COTS user hardware and software found in most offices, schools, and homes. This technology is then combined with an underlying host operating system, virtual machine monitor, virtual network hubs, network encryptors, and a filtering router that allows multiple machine environments to run simultaneously and to access multiple networks all from the same physical platform.

## *WIDS: Wireless Intrusion Detection System*

*Wireless Local Area Networks (WLANs) are exploding in popularity as users demand greater mobility. They are widely used in industry, government, and homes around the globe. WLANs are convenient but unprotected, and their reliance on open, uncontrolled transmission medium makes them highly vulnerable to attacks and intrusions.*

The U.S. Defense Department now mandates that all DoD WLANs be protected by Wireless Intrusion Detection Systems or WIDS at all times to mitigate risks and provide a more secure operating environment. The problem, however, is that even the best detection systems are not effective enough to protect secure or classified networks. To address this problem, researchers at NSA have developed a new approach to detect intrusions on wireless networks. This new approach is consistent with many of the DoD requirements for WLANs security.

WIDS detects rogue access points and clients, rogue devices actively communicating with valid devices, ad hoc and bridged networks, deviations from network security policy, packet flooding denial-of-service attacks, MAC spoofing, and frames having 802.11 protocol violations.

NSA's innovative system can also determine the channel that a packet is transmitted on, which is a big advantage over other WIDS that only detect the receiving channel. Users can also customize NSA's tool to create custom capture filters and attack signatures. WIDS has the ability to simultaneously and continuously monitor all 802.11 channels.

## *Testing a Wireless Device*

*The evolution of wireless devices has taken consumers by surprise and the use of wireless devices have proliferated throughout the world. 802.11 wireless devices, such as cell phones, cameras, and MP3 players all connect to the internet using a wireless open, uncontrolled transmission medium.*

Researchers at NSA have found a way to allow users to test their wireless devices for security weaknesses and proper functioning. This method tests the device by generating network traffic packets that may be properly formatted, improperly formatted, or partially formatted. The user may configure the header or payload either directly, through a program, or from a file. The configured frames may be transmitted for a user-definable number of iterations or set for continuous transmission in a repeating manner. After all of the frames are sent, at least one statistic about the wireless device under test is provided to the user.

## *Stepping Stones*

*When hackers attack a computer, they frequently use one or more intermediary computers to hide the location of the attacking computer. These intermediary computers are called "stepping stones". Researchers at NSA have developed a new tool that detects computer attacks and the involvement of a "stepping stone" in the attack. This method may be incorporated in a tool to search for the location of the attacking hacker.*

NSA's method uses data passively collected from the network and cannot be detected by a hacker watching for possible countermeasures to his attack. After collecting the data, this method filters out and compares latency times from different layers of the data for a specified set of communications. If the latency exceeds a specified threshold, an alert is sent to the network or computer security analyst. The analyst may adjust the collection parameters, data filtering parameters, and the alert latency threshold. If the tool indicates that there is a "stepping stone", it can determine how near or far it is from the attacking computer. Computer analysts can use this information to help them locate the hacker.

## *TRICKLER*
## *Analytic Metadata Producer*

*Companies who rely on the internet to market their goods and services need to understand how potential customers use the web to search for information. Research scientists at NSA have developed a new process that can help them do that.*

TRICKLER monitors internet surfing habits and history, formats the resulting data, and sends it back to a central database for further research. TRICKLER combines an advanced data aggregation methodology with open source vulnerability information, operating system fingerprinting technology, and statistical methods to detect host and network attributes. It efficiently collects repetitive portions of network data, then correlates and analyzes the results to identify surfing trends and network assets.

*We must continue to explore, understand and exploit the power of advanced mathematics.*

In order to remain a world leader in cryptologic methods, NSA must maintain our knowledge base of advanced mathematics to secure U.S. communications and maintain the country's ability to exploit new advanced foreign communications systems.

NSA mathematicians are involved in a broad spectrum of sub-specialties, from algebra to statistics, and number theory to combinatorics. Many of the projects are interdisciplinary, requiring interaction with computer science, engineering, and linguistics technical experts.

NSA provides individual grants and conference funding in support of advanced mathematics research through its Mathematical Sciences' Program. The Director's Summer Program and the Mathematics Education Partnership Program were created in order to encourage future mathematicians, award grants for relevant mathematics research and offer bi-directional sabbaticals. Whenever possible, NSA continues to share mathematical insights with its partners in academia and industry.

Additional information on specific technologies involving Advanced Mathematics can be obtained by contacting the TTP Customer Service Center at 443-445-7159.

*We remain at the forefront of advanced computing research and development.*

NSA's state-of-the-art computing infrastructure has maintained the development of secure cryptographic algorithms for U.S. communications and the exploitation of foreign communications. Today, we remain committed to the computer sciences and attract some of the brightest computer professionals in the nation.

NSA relies on a vast network of advanced computing resources in order to collect, sort, process, and analyze the raw data that produces foreign intelligence. Our current needs span several computing disciplines, including scientific programming, modeling, engineering, signals processing, graphical user interfaces, secure computing, text processing, database sorting and retrieval, artificial intelligence, and neural networks.

Cooperative efforts with universities and private industry are pushing NSA's supercomputing capabilities even further. NSA is dedicated to sharing its computing advancements with commercial enterprises via technology transfer.

## *Quantifying Digital Voice Enhancements*

*Researchers at NSA have developed a new statistical method of detecting duplicate voice recordings that doesn't require a human listener or phonetic transcription systems. This technology is both language and content independent.*

This technology processes the unique pitch contour of the human voice and extracts specific statistical parameters that are used to create a numerical fingerprint of the voice in a computationally efficient and readily implementable way.

Potential markets for this technology include voice recording libraries, personal surveillance systems, repetitive voice messaging, and nuisance call detection. An anti-spoofing application is also possible for use in biometric voice verification systems.

*The NSA is aggressively leading research efforts.*

Advances in communications technologies increase the complex set of speech, data, video and multimedia signals, and the need for comprehensive information processing techniques. NSA is aggressively leading research efforts in these directions and applying new advances to the collection and processing of various forms of communication and the protection of communications among U.S. government organizations, including military, defense, and non-defense agencies.

Commercial applications of NSA's information processing technologies include efficient techniques for secure mobile communications, cutting-edge machine learning technologies, and high-speed, wide-bandwidth, multi-media signaling. NSA's information processing expertise has made a significant contribution to industry and will continue to further the nations competitiveness within the global economy.


## *Aladdin Tool Suite: Name Matcher and Tagger*

*Searching through large volumes of multi-lingual information to retrieve specific data, particularly names, is an important challenge for both government and industry. This difficulty escalates when non-western languages, such as Arabic, are transliterated into a romanized alphabet.*

Aladdin Tagger first searches for transliterated names and is effective even within large data. It finds and marks up any matches using an automated expert system that looks for various identifiers and culturally specific, non-western personal names embedded in the native script. Non-experts can effectively conduct expert searches for transliterated names in large data sets and do so taking advantage of the best available linguistic rules.

This knowledge-based system for name matching and tagging is maintained with contributions from expert linguists and contains an extensive collection of transliterated-names data. Its ranking algorithm uses relative frequencies of spellings in large data sets to highlight most likely matches.


## *Nellauger: Generating Transliterated Names*

*Transliterated Names is the challenging process of taking a word or text written in one language and converting it into the alphabet of another. Experts using conventions can build sets of transliterated names, but the results can vary greatly with wide differences of spellings – especially with non-western names.*

Transliterated Names is an automated transliteration system developed by NSA that meets these challenges. An additional benefit of automated transliteration is the ability to build and maintain knowledge bases of plausible spelling variants of transliterated names.

These knowledge bases are easily searched. They are used to support valuable tools for those who need to match transliterated names in large data sets – even for non-linguists who do not type or recognize the native script. Non-linguists can also transform all or part of a native script text into standard romanized spellings that can be easily searched. Transliteration is immediate and the results appear while entering text.


## *RENOIR: General Network Visualization and Manipulation Program*

*Analysts in a wide variety of disciplines need be able to look at large volumes of data, quickly discard irrelevant information, and identify interesting relationships. NSA's Renoir is a versatile and highly developed software tool that can do just that.*

Renoir takes large data sets that would otherwise be difficult for users to conceptualize and turns them into easily readable graphs. This powerful visualization tool works on any data set that contains associations and allows data from a variety of sources to be shared. Renoir's unique patented data layout, community clustering algorithms, and well-developed Graphical User Interface allows users to manipulate, analyze, and customize the tool. Renoir is written in Java to run on any platform supporting the Java Virtual Machine.

Renoir is ideal for business intelligence applications and can be tailored to meet the needs of specific industries. Potential markets include bioinformatics, law enforcement, energy management, telecommunications, finance, marketing, data mining, customer relationship management, knowledge management, business performance management, statistical analysis, and search engines. This government owned software is available for use by any government agency.

## *Topic Determination of Textual Information*

*NSA has a new invention that overcomes the problems of common keyword-based searches for document retrieval. Common keyword-based searches often lead to over-specification or over-generalization, especially when searching a large number of documents or executing numerous queries.*

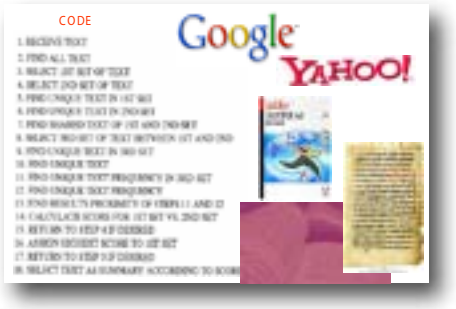
NSA's technology, in contrast, generates a topic description and categorizes sample text, then searches and sorts new text by topic. The text may be of any length, in any language, and may be derived from any source, to include machine translated speech or an optical character reader.

This approach is effective for searching and sorting text by topic without using keyword proximity, n-grams, or Boolean combinations of keywords. It does not require stop lists or extensive stemming. Document retrieval by topic is more accurate and has the added advantage of providing an automatic maintenance scheme. Without automatic maintenance, large-scale knowledge bases degrade and become inoperable in today's dynamic environment.


## *Text Extraction from Color Images*

*Today's search engines and scanners do a great job of processing text alone, but they are powerless when that same text is embedded in a color image. This is a significant limitation for search engines in today's internet age since text often appears in photos, videos, and full color graphics, such as maps and charts.*

NSA has developed a patented suite of algorithms that can detect and extract text from any image, including photos, maps, and videos. The extracted text can then undergo further automated processing by an optical character reader or a search engine. This highly flexible set of algorithms uses simple math and can extract text in any shape, form, language, or location from a color image of any size or format. It digitally separates the text from the image in a sequence of parallel operations. Law Enforcement agencies could use this methodology to search through traffic footage to find license numbers of speeding motorists. Intelligence Community agencies could use it to search for hidden threats in on-line photos and maps. Search engine companies could upgrade browsers to search images for text. This powerful tool can be custom-tailored by the user for optimal results.




## *Summarizing Text Using Just the Text (KODA)*

*Today's search engines and content managing systems often rely on dictionaries, encyclopedias, or exemplary texts to navigate and search through data. These tools work well until they are applied to large volumes of information. A research team at NSA took up this challenge and found a new way to search through and navigate large volumes of data.*

KODA uses the text itself to search and navigate large sets of data, not dictionaries or encyclopedias. It works by measuring the similarity between passages of text and selects sentences it can use to summarize the text. KODA performs well on large data sets in many languages regardless of formatting. It can read thousands of documents and publish a summary of user-definable length for each document. It can also read web pages and complement search engines by summarizing the content on the page in which a keyword appears. Overall, KODA is an ideal application for integration into search engines and content management systems to address the expanding problem of information overload.

## *Note Enhancement: Retrieving Electronic Data During Note Taking*

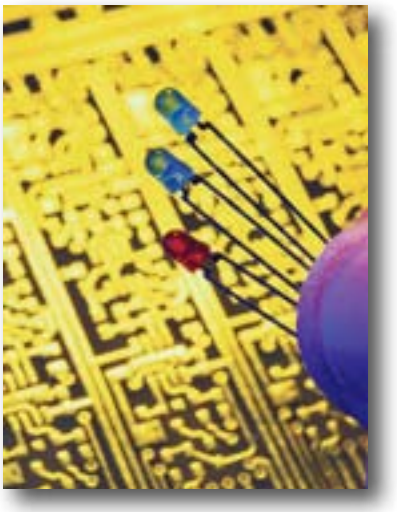
*Note taking applications for wireless devices are becoming widely used to keep information clean and organized. People use these applications to jot down phone numbers, things-to-do lists, messages and meeting notes to become more productive. NSA Researchers have developed an existing enhancement to complement these applications.*

NSA Note Enhancement allows a user to retrieve information in near real time from the internet or on-line databases while taking notes. This invention combines several existing “smart pad” technologies and wireless technology to automatically capture and extract information from written notes, while connecting to a search engine application or database. Users are also able to customize their keyword searches to request additional information and receive responses in real time.

*We actively encourage research and development activities within this field.*

NSA develops new designs and refines fabrication technology for complex, sub-micron feature-size integrated circuits that are usually highly classified and produced in small, cost-efficient lots. At the Laboratory for Physical Science, researchers continue to pioneer techniques in several areas related to microelectronics research.

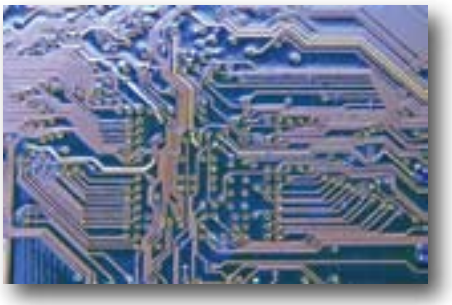
The NSA microelectronics community maintains a cooperative relationship with the U.S. semiconductor industry. This effective interaction results in opportunities for NSA and industry to evolve, maintain, sustain, and advance the U.S. microelectronics industry.



## *Low Cost Single Die-Level Plating Process for Integrated Circuits*

*Today's integrated circuits are the building blocks of almost every modern electrical device from cars, computers, television sets, CD players, telephones, and cameras. Micro-electronics packaging industries, national laboratories and universities are interested in lowering the cost of fabricating these circuits and reducing production time. A research team at NSA has found a way to do both.*

NSA's new process for packaging integrated circuits does not require expensive and time consuming electroplating equipment. The technology allows the aluminum bond pads on the circuits to receive solder, eliminating the need for wafers, masks, several lithography steps, sputtered metal deposition, or electroplating. The result is large volumes of single-die level and wafer-level plating done without electroplating. A group of up to 50 die can be plated in less than one day as compared to 10.5 days for a wafer-level electroplating process.

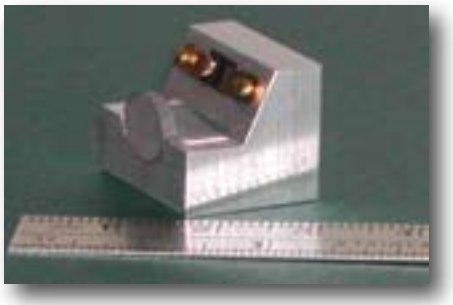


## *Fabricating Very High Density Double-Sided, Multi-Layered, Flex Interconnect*

*Consumers today demand smaller electronic devices with even greater functionality: tiny cell phones that store music, access the web and take photos, MP-3 players for songs, games, videos, photos, and internet access. These higher performing smaller devices require high density, high performance, low profile circuitry that can overcome strict electrical and physical constraints.*

The circuitry required must have low electrical resistance, low cross-talk, and high operating frequency. It must have a low enough profile to physically fit into smaller devices. The wiring density of the system level interconnects must keep pace with the rapidly increasing number of Input/Output connections on the chip.

NSA has found a way to meet these challenges with a new technology that enables the fabrication of very high-density, double-sided, multi-layered circuits. The process combines semiconductor processes at high temperature with releasable bonding techniques. The superior electrical and physical characteristics of the circuits created using this technology address the electrical and physical constraints of portable electronic devices.



## *Forward Scattered Electronic Image (FSEI) Sample Holder*

*Nearly all labs have a Scanning Electronic Microscope (SEM), yet relatively few have the high resolution Transmission Electron Microscope (TEM) due to its cost. The FSEI sample holder uniquely brings near-TEM quality to the SEM by providing information about the sample that is both surface sensitive and very high resolution. The sample is simply mounted to the holder and placed in the microscope.*

There is no need to add any extra detector hardware to the microscope's chamber. The incident electron beam intercepts the sample at a shallow angle and the resulting forward scattered electrons are directed towards a target which emits secondary electrons that are then counted by the microscope's standard secondary electron detector. The collected signal is higher resolution and more surface sensitive than secondary emission, and this results in images with well-defined, three-dimensional appearances, allowing resolution in the 1.0 nanometer range.

The sample holder provides significant improvement from the typical SEM resolutions of several nanometers from using secondary electron imaging. This new technology enables superior high-resolution imaging on a general category of samples and eliminates the need for additional hardware at a significant cost savings.

## *Three-Dimensional Microsystem and Fabrication Method*

*As consumer demand for smaller, multi-functional electronic devices escalates, industry requires a more economical approach to miniaturization. In response to this challenge, NSA has developed a way to fabricate the integrated microsystems needed for miniaturization in a more cost effective manner.*

NSA's approach reduces the cost of building ultra-miniaturized microsystems by using COTS components and by streamlining the fabrication process. Passive elements, such as filters and capacitors, can be made using optimized substrates, rather than more expensive silicon. By performing functional quality control tests at multiple points in the process, production output increases. This cost-effective approach to miniaturization provides an opportunity for micro-integration of optical and mechanical devices with electronics and COTS components. Potential applications include remote environmental sensors and networked control systems within industrial facilities.

**COTS** - Commercial Off The Shelf

**CRADA** - Cooperative Research and Development Agreement

**EPA** - Education Partnership Agreement

**FLC** - Federal Laboratory Consortium

**IAM** - Intellectual Assessment Management

**IP** - Intellectual Property

**OGC** - Office of General Counsel/Intellectual Property and Technology

**OM** - Opportunities Management

**PLA** - Patent License Agreement

**R&D** - Research and Development

**TTAP** - Technology Transfer Assessment Panel

**TTP** - Technology Transfer Program

**TTSA** - Technology Transfer Sharing Agreement

# NSA Technology Transfer Program

National Security Agency, 9800 Savage Road, Suite 6541, Ft. Meade, MD 20755-6541
www.nsa.gov/research/tech_transfer