Preparation for the launch of PeopleSoft v9.0

An overview of the coming changes and how they affect you

On Monday, June 21, Sandia will launch the much-anticipated upgrade to its human resources information system, known as PeopleSoft. This upgrade is designed to introduce a modernized, simplified PeopleSoft system that serves the Labs' Human Resources functions in the most efficient, simple, and cost-effective ways possible. In the new system, PeopleSoft users will see changes in both appearance and functionality and help is available to guide users through this transition.

In conjunction with the information that has

(Continued on page 6)

upgrade

Cyber bad guys get smarter, Sandia defenses get stronger

How to counter both known and unknown threats

The Lab News *recently interviewed three members of Information Technology management: Chief Information Officer Art Hale (9600), Acting Director of Computing & Network Services 9300 Tom Klitsner (who is also senior manager of Computer Support Unit Services 9340), and Carol Jones, senior manager of Cyber Security Services & Technologies 9310.*

* * *

Lab News: *We frequently hear that the cyber threat is significantly more serious than a decade ago. What's worse about it? Why is this a more dangerous environment?*

Art Hale: A lot of people have learned a lot of things over the past decade. Software designers have learned how to create better software, and the people who want to exploit our current operating environment have also learned a lot about its weaknesses, its vulnerabilities, how to attack it and compromise it.

LN: *Are you talking about people we usually call hackers? High school or college students doing it for fun?*

Art: I'm talking partly about them, but a more serious threat to Sandia's work environment is nation-state adversaries that target a place like Sandia because of the kind of work we do, nuclear weapons and other national security applications. They're interested in our most sensitive information. They use all the mechanisms at their disposal to try to find out as much as they can. So we're facing very sophisticated attacks.

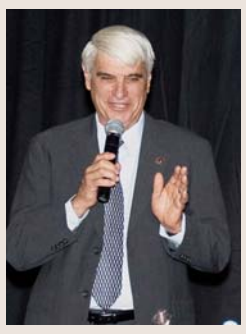
The second thing that has happened in the past decade is that much of what we do has moved to the Internet. People need to interact across the Internet, they need to find and access information over the Internet. They find it from all kinds of places using search engines, and the adversaries who want to attack us know that and exploit it. They can compromise machines elsewhere that have information that we might be interested in — we may just happen there, or there may be something that's close to us. An employee of Sandia might access the website of a local TV station, or something at a university near by, for example.

(Continued on page 5)

See also . . .

Peeling the onion of malware: A Laboratory Directed Research and Development (LDRD) project to understand and develop countermeasures for malware and botnets. **Page 3.**

Bright future for cloud computing: What is cloud computing, and what might it mean for Sandia? **Page 5**.



Notable New Mexican Sid Gutierrez

Former astronaut and longtime Sandian **Sid Gutierrez** (4100) was named the 2010 Notable New Mexican by the Albuquerque Museum Foundation. Read about the award in a story on **page 12.**

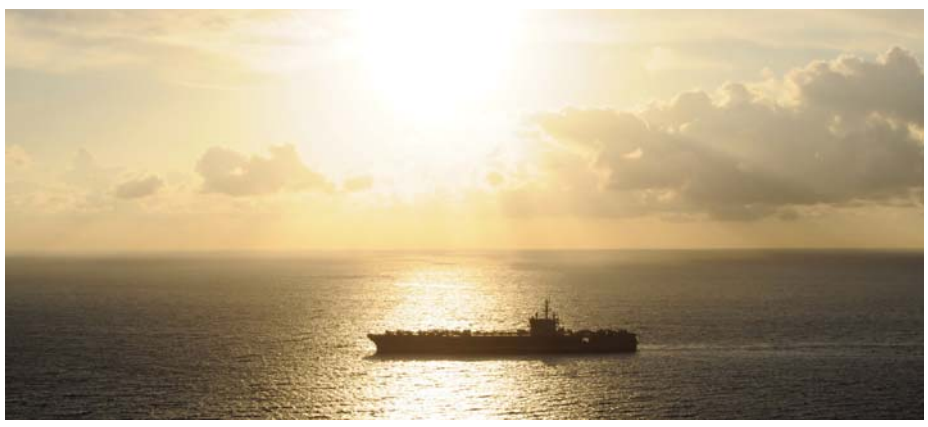
Sandia LabNews

Vol. 62, No. 11 June 18, 2010

Managed by Lockheed Martin for the National Nuclear Security Administration

Sandia National Laboratories

Admiral's talk explores security implications of climate change



IT'S A NAVY THING — Oceanographer of the Navy Rear Adm. James Titley tells Sandia audience the US Navy is concerned with climate change because rising sea levels could threaten port facilities around the globe. (US Navy photo by Senior Chief Mass Communication Specialist Spike Call)

CNSAC speech links with new Sandia research direction

By Neal Singer

The US Navy views climate change as a challenge, intends to prepare for it, and would appreciate help from the national labs, Rear Adm. David Titley told an attentive Sandia audience in an unclassified lecture titled "Climate Change and National Security" on June 2 in the Bldg. 810 (CNSAC) auditorium.

The lecture, simulcast to Sandia/California, is the first of a group of lectures intended to explore the national security implications of climate change, says Rob Leland, director of Computation, Computers and Math (1400), whose center arranged the talk under the leadership of John Mitchiner (1430) through Div.8000 VP Rick Stulen's Energy, Climate and Infrastructure Security SMU.

Titley, the Navy's oceanographer and navigator, is senior policy adviser to the chief of naval operations for issues relating to national ocean policy and governance, as well

(Continued on page 4)

State of the Labs 2010

PASSING THE TORCH — Labs Director Tom Hunter, left, and Paul Hommert, who will become Sandia president and Labs director on July 9, answer questions from the media ahead of the 2010 State of the Labs presentation at the National Hispanic Cultural Center Tuesday evening. Tom talked about the challenges of maintaining the nuclear weapons stockpile, cyber security, terrorism, energy, and economic competitiveness. He then turned the presentation over to Paul, who discussed an "exciting" future for Sandia as its mission diversifies and paid tribute to Tom. More in the next *Lab News*. (Photo by Lloyd Wilson)

Inside

That's that

I'm a bit of a word buff — Who knew, right? — and always get a kick out of watching the language evolve. I find English remarkable in its adaptability and flexibility. It seems to me that there's a deeply pragmatic strain hardwired into the DNA of the language (Am I mixing metaphors there?) that says, if a word works, take it, use it, and make it your own regardless of its national origin. Not being bilingual or multilingual, I don't know the extent to which other languages are as easy in their virtue as is English. Maybe lots of them are. Spanish speakers incorporate English words into their conversation all the time, for example.

But thank goodness we don't have the equivalent of the *Académie Française*, which for three centuries has been fighting the good fight to keep French free of foreign — and especially English — contamination. Incredibly, the results of its deliberations are published as official laws, laxly enforced, to be sure, but still. (All we have is those seven words you can't say on TV.)

Here's one of the things I like about my native tongue: We don't just borrow words from other languages . . . we make them up with dizzying abandon.

What brings this up? In my role as editor of the *Lab News* I use *The Associated Press Stylebook* a lot; it's the bible of style and usage in the news business: When do you capitalize the word "president?" How do you set off the title of books? Should a.m. and p.m. have periods? For a wordaholic the stylebook is endlessly fascinating. I actually find myself reading it for pleasure sometimes. (I know. I know.)

The other day, I got an email from AP. Periodically they send out notes updating usage and style questions. This note provided a list of words related to social media. (AP by necessity has to keep up with the language as it is actually used and spoken, of course.) Among the words: metadata, retweet, unfriend, crowdsourcing, wiki. Even familiar words have new meanings and usages: fan, follow, avatar, handle.

We have all these words to talk about things that didn't even exist a decade ago and now they're totally assimilated into our society.

There's a lesson here: when something is useful — the web, or social media, for example — people will embrace it and use it, and create a language around it, and it will be very, very difficult to make them stop. Once Facebook enters the language, it ain't going anywhere. The converse is probably true, too: If something isn't useful, it's probably going to be very hard to make people adopt it.

That's why the French language police are always fighting a rearguard action: French speakers find certain English words useful . . . and they use them, language purists notwithstanding. I do sympathize with the effort, though. Perhaps it's time for a "*rapprochement*" with our French-speaking cousins: we won't use any of their words if they don't use any of ours. *Détente* anyone? *Mais oui!*

* * *

One of the hardest things we do — and I think one of the most important — is to publish obituaries about on-roll employees who pass away. I call them "obituaries," but they're probably better described as memorials. We don't try to provide a comprehensive summary of an individual's life; rather, we offer a forum where colleagues and friends can offer a few remembrances. We've been told the memorials mean a lot to coworkers, who often feel like they've lost a member of the family. And perhaps it's not surprising that surviving family members often consider *us* — fellow Sandians — as members of a big, extended family. Case in point: Rose Salas, sister of Fred Salas, who passed away March 12, sent a very nice letter to the entire Sandia workforce. I'm glad her note found its way to my desk. Here are some excerpts from what Rose wrote: "I would like to take this opportunity to express my sincere and deepest gratitude in how my brother Fred Salas was treated by what I will always refer to as his professional and caring work family. . . . Each of you was considered family by Fred. I know he looked forward to work every day knowing that he would be surrounded by those who meant so much to him. . . .[H]e spoke of work often, never about what he did, but about the people he was surrounded by. . . . Thank each of you for all you did for him as coworkers and friends. I also remain grateful to Sandia Laboratories for being an important part of why Fred was able to enjoy his life to the fullest. . . . Each of you made our loss a bit easier in returning to us that huge caring smile that Fred shared with you at both his rosary and his funeral. Fred looked down to see his WHOLE family together."

See you next time.

— Bill Murphy, (505-845-0845, MS0165, wtmurph@sandia.gov)

Sandia LabNews

Sandia National Laboratories

http://www.sandia.gov/LabNews

Albuquerque, New Mexico 87185-0165
Livermore, California 94550-0969
Tonopah, Nevada • Nevada Test Site • Amarillo, Texas • Carlsbad, New Mexico • Washington, D.C.

Sandia National Laboratories is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin company, for the US Department of Energy's National Nuclear Security Administration.

Bill Murphy, Editor **505/845-0845**
Randy Montoya, Photographer **505/844-5605**
Mike Janes, California site contact **925/294-2447**
Michael Lanigan, Production **505/844-2297**

Contributors: Neal Singer (845-7078), Iris Aboytes (844-2282), Patti Koning (925-294-4911), Stephanie Holinka (284-9227), Karyn Scott (284-8432), Darrick Hurst (844-8009), Stephanie Hobby (844-0948), Heather Clark (844-3511), Michelle Fleming (Ads, Milepost photos, 844-4902).

Lab News fax **505/844-0645**
Classified ads **505/844-4902**

Published on alternate Fridays by Media Relations and Communications Dept. 3651, MS 0165

LOCKHEED MARTIN

Lab News Reader Service

The *Sandia Lab News* is distributed in-house to all Sandia employees and on-site contractors and mailed to all Sandia retirees. It is also mailed to individuals in industry, government, academia, nonprofit organizations, media, and private life who request it.

Retirees (only):

To notify of changes in address, contact Benefits Dept. 3332, Customer Service, at 505-844-4237, or Mail Stop 1021, Sandia National Laboratories, Albuquerque, NM 87185-1021.

Others:

To receive the *Lab News* or to change the address (except retirees), contact Michelle Fleming, Media Relations and Communications Dept. 3651, 505-844-4902, email meflemi@sandia.gov, or Mail Stop 0165, Sandia National Laboratories, Albuquerque, NM 87185-0165.

Employees:

To address concerns regarding delivery of the *Lab News* to your facility, call Mail Services Team 10268-4, at 844-3796. At Sandia/California contact the Mail Room at 925-294-2427.

Web users:

The *Lab News* is on the external web at www.sandia.gov/LabNews. *Lab News Interactive*, accessible on the internal web, is at: www-irn.sandia.gov/newscenter/interactive.

TVC

Entrepreneurial seminars offered

Seminars are being offered this summer to Sandians who want to broaden their entrepreneurial skills and learn how to commercialize their technology-based innovations.

Technology Ventures Corporation's Center for Commercialization & Entrepreneurial Training (CCET) in partnership with DOE, Lockheed Martin Corp., and Sandia's Intellectual Property Management, Alliances and Licensing is sponsoring the seminars on Thursdays starting June 24 in building 858EL/L1410 from 11:30 a.m. to 1 p.m.

The course titles, topics, and dates are:

June 24: **Technology Transfer Practices** introduces the entrepreneurial services of Sandia and Technology Ventures Corporation (TVC).

July 1: **Entering the Entrepreneurial World** introduces the concepts and issues of commercializing a technology-based product, and analyzing the business and financial potential of a product.

July 8: **Preparing and Presenting the Business Plan** takes the entrepreneur step by step through the process of developing and writing a business plan directed toward achieving equity financing for his/her innovation and company.

July 15: **Break.**

July 22: **Market Research and the Marketing Plan** discusses the significant endeavor in determining the market potential of a product, understanding the dynamics in the marketplace, and producing a marketing plan.

July 29: **Financial Management** explores raising capital, understanding and using the financial statements, preparing budget projections and proforma financial statements, and company valuation.

Aug. 5: **Operations Startup and Organization Structure** describes the business organization development process and the essential legal, accounting, taxation, and securities issues.

Aug. 12: **Attracting Equity Investors and Lessons Learned** discusses the developing relationships with investors and intellectual property. We will also gain the benefit of hearing from those individuals who have experienced the equity funding process.

Lunch will be served at the classes. The seminars are free of charge, but please RSVP to Margaret Speer at 843-4202 or margaret.speer@lmco.com.

Sandian appointed examiner for 2010 Malcolm Baldrige National Quality Award

Joshua Parsons (10610) has been appointed to the 2010 board of examiners for the Malcolm Baldrige National Quality Award, the highest level of national recognition for performance excellence that a US organization can receive.

JOSHUA PARSONS

As an examiner, Parsons is responsible for reviewing and evaluating applications submitted for the award. He was appointed by Patrick Gallagher, director of the Commerce Department's National Institute of Standards and Technology.

Parsons is a business administrator for Division 1000. Later this month, he will transfer to 10629 to be Center 2900 business manager. He also has served three terms on the Quality New Mexico Board of Examiners, a nonprofit organization that encourages quality in businesses and other organizations.

The board is composed of approximately 500 individuals from industry, professional, education, health care, nonprofit, and trade organizations. Those selected meet the highest standards of qualification and peer recognition.

The Baldrige Award may be given annually in each of six categories: manufacturing, service, small business, education, health care, and nonprofit.

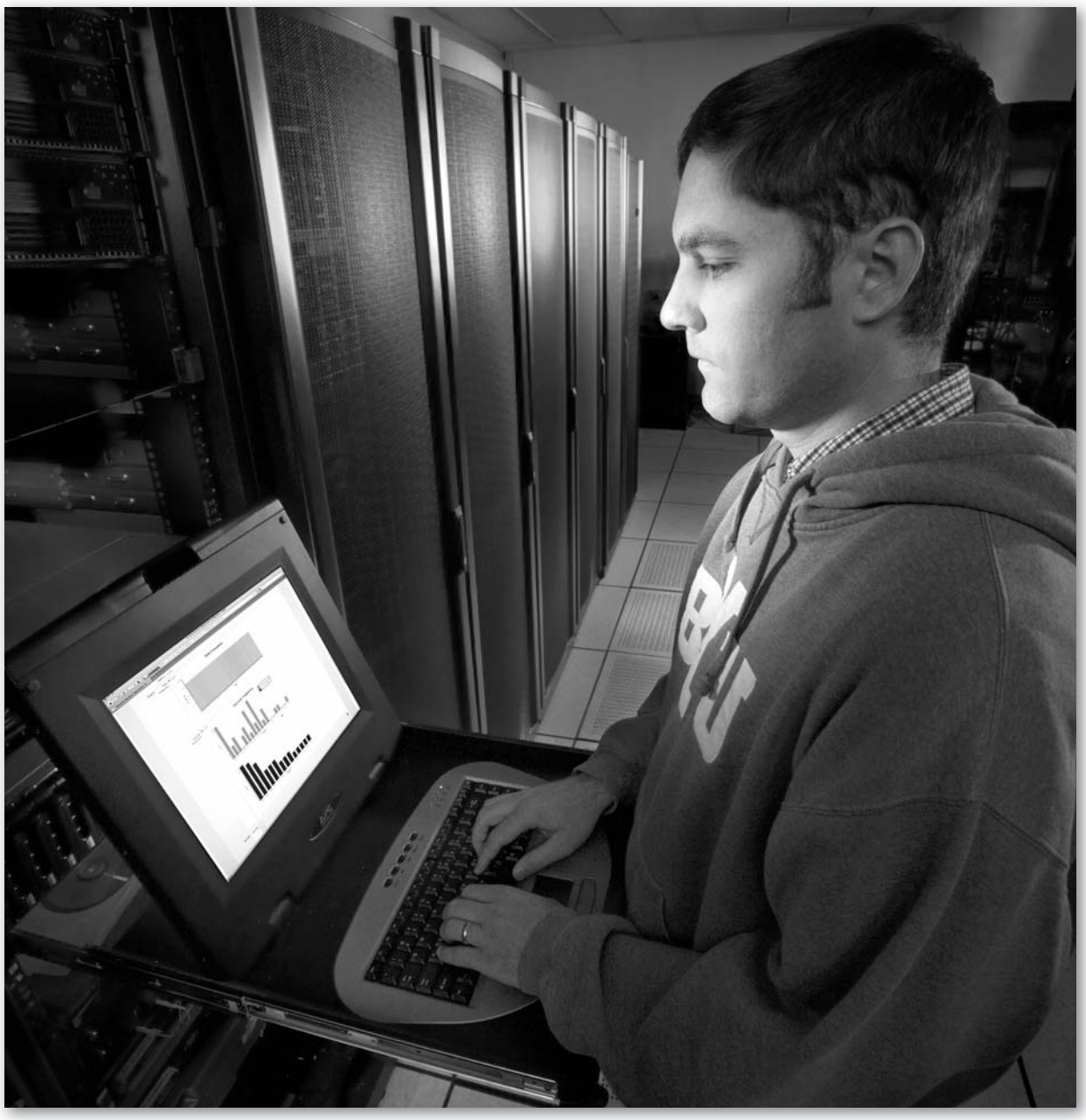
Information about the Baldrige National Quality Program and the application process is available by contacting the program at (301) 975-2036 or nqp@nist.gov, or from the program's website at http://www.nist.gov/baldrige.

Retirements

Retiring and not seen in the *Lab News* pictures: Dolores (Dolly) Yoder (10667), 45 years; Anne Weimer (5001), 19 years.

Peeling the onion of malware

Sandia CaliforniaNews



THE FORENSIC ANALYSIS REPOSITORY FOR MALWARE (FARM), created by Jamie Van Randwyk, Ken Chiang, and Levi Lloyd, enables computer security personnel to triage malicious software within minutes, giving them an advantage in the fight against cyber attacks. Here Levi examines FARM's analysis of a variant of the Waledac botnet. (Photo by Randy Wong)

By Patti Koning

Sun Tzu said it first, in the sixth century: "Know thy enemy." In *The Art of War*, Tzu writes that to be successful (or to win 100 battles, in some translations), a warrior must know himself and his enemy. This proverb applies to military strategy, sports psychology, and internet security.

For the past three years, Jamie Van Randwyk, Ken Chiang, and Levi Lloyd (all 8965) have been working on a Laboratory Directed Research and Development (LDRD) project to understand and develop countermeasures for malware and botnets (see "Malware 101 and botnets, too" at right). To streamline the work of sifting through thousands of instances of malware, they developed the Forensic Analysis Repository for Malware (FARM), a tool that, as Jamie puts it, has taken on a life of its own.

Looking at each individual piece of malware would take an experienced computer security analyst like Ken or Levi anywhere from 30 minutes to a couple of hours. With FARM, that process is fully automated and takes about five minutes.

"FARM enables malware triage in a true triage timeframe," Jamie says. "Many government institutions only have a handful of highly skilled analysts, so their time is precious."

Jamie describes FARM as a basic framework with a nice web interface on the front end, an extensive database on the back end, and a number of hardware resources. Users then plug software resources into the framework, so the tool is fully customizable — for example, one could run separate unclassified and classified versions — and easily upgradeable, an important feature for keeping pace with malware developers. Most of the software resources already existed and were readily available; the key to FARM is harnessing the software resources together with the database.

Ken and Levi, in addition to their research, work in computer security. From that perspective, they immediately saw the practical application of FARM. The tool is now being used across Sandia and at a number of other government agencies.

"As more people use FARM, we can take what they learn and continue to improve the entire package," Jamie says.

The team chose to investigate Storm and Waledac, two complex, pervasive, and long-lasting botnets. Storm is said to have been responsible for up to 20 percent of the world's spam at its heyday, infecting up to a million computers by some estimates. Waledac, considered by many to be a second iteration of Storm, infected hundreds of thousands of PCs worldwide and was thought to be capable of sending more than 1.5 billion spam messages a day. Through its Digital Crimes Unit, Microsoft Corporation effectively shut down Waledac last year, a major victory over the malware underworld.

To get at the core of the malicious software, Ken painstakingly worked to defeat multiple protection mechanisms. "The amount of work is asymmetrical," he explains. "It's easy to put on the protection mechanisms, but it takes a tremendous effort to take it apart."

To reverse engineer the malware, Ken used three different technical approaches: static analysis, dynamic analysis, and emulation. Malware authors wrap their code in defensive layers both to obscure their true purpose and prevent reverse engineering. For example, a code may not run linearly, meaning it jumps around seemingly randomly among a million lines. Or, designers modify a program so that parts of the code modify other parts so that its real purpose is not readily apparent. Some malware is designed to detect when it is being run and watched, and alter its behavior.

The researchers learned that quickly disabling protection mechanisms is a key step to understanding and stopping the spread of malware. Ken can now unwrap a piece of malware in about a week, a process that took several months at the start of the LDRD. He's beginning a late start LDRD that aims to use FARM to automate that unwrapping process — an "everything-but-the-kitchen-sink" tool that would be integrated into FARM.

After three years studying botnets on a small scale — from one to 40 hosts — the researchers now want to look at the other end of the spectrum. "We're proposing a new LDRD to boot a million windows nodes and study large-scale behavior of bots," Jamie says. "Things happen at that scale that you just can't see even with 10,000 instances."

The work builds on research led by Ron Minnich (8961). Last year, he demonstrated the ability to run more than a million Linux kernels on virtual machines (*Lab News*, July 31, 2009). The researchers plan to take two approaches: emulating the properties of a Windows system sufficiently to run in a large-scale environment and reducing the size of Windows. "The size of Windows is a significant hurdle in getting to a million nodes," says Jamie. "Right now for every 10 instances of Windows, you could probably boot a thousand instances of Linux."

He's hoping that this research may unlock a new approach to combating malware. "Until there is a fundamental change in the way we do computing — something huge like no longer using the Intel architecture — malware and malicious software are a fact of life," Jamie says. "There have been lots of good, incremental changes, but we're looking for a game changer. Automating the process of stripping protection mechanisms might be one. Looking at a Windows botnet from the vantage point of command control could reveal other approaches."

Malware 101 . . . and botnets, too

Malware is short for malicious software, a term that encompasses what is commonly known as computer viruses, worms, Trojan Horses, and spyware. Over the past 20 years, computer viruses have gone from being annoying — in some instances, more akin to graffiti tagging — to downright lethal.

Not coincidentally, that's the same time frame in which the Internet went from being limited to universities to being ubiquitous. According to the website Internet World Stats, in 2000, 3.6 million people used the Internet; as of September, that number had jumped to 1.7 billion.

Malware is ubiquitous and moves at lightning speed; it is common for a newly installed computer running Windows XP to be infected within 10 minutes of being connected to the Internet.

Once installed on a user's computer, malware is used to collect information about the user's behavior, which can be used to display intrusive pop-up ads or record keystrokes to steal passwords and other sensitive information. Or, malware can be used to turn a computer into a zombie. Unbeknownst to the user, a zombie computer (a more technical term is "compromised computer") is used as part of a larger network of like computers (hence the term botnet, for robot network) to wreck havoc on the Internet.

"In the early days, hackers seemed to be writing malware more for bragging rights about how many computers their virus could spread to and how quickly. Today, there are financial reasons to spread malware and build the largest possible botnet," Ken explains. "There is an underground economy built around botnet 'owners' renting their botnet to the highest bidder, who might use it to blackmail a company by threatening to take down its website."

The organized crime element of the botnet world has led to a curious Wild West environment on compromised computers. Recently, Ken's father suspected his computer might have been compromised and asked him for help. Ken found that the computer was indeed compromised many times over.

"His computer was essentially a battlefield, with 80 different viruses fighting it out for control," Ken says. "Malware is now being written to not only take control of a computer, but defeat any other malware that is already there doing the same thing."

Despite the "Whac-a-Mole" nature of combating malware, Ken thinks Sandia's efforts, along with the efforts of many others in the field, are making serious inroads. And, he finds the work very gratifying.

"For every defensive rule we can come up with, the bad guys find an exception around it," he explains. "But the silver lining is that as we come up with different practices, the whole of the practice improves and we are slowly but surely making life harder for the malware guys." — *Patti Koning*

A new approach to energy security

By Shannon Guess (12150)

"Creating Focus in Turbulent Times." That is the theme of Sandia's FY 2010 Strategic Plan, a theme exemplified by the challenges the nation faces in a wide range of energy-related issues.

Consider: The US today is confronted with an unprecedented environmental crisis in the Gulf of Mexico, relentless cyber attacks threatening the electrical grid, foreign oil expenditures weakening the national economy while directly funding US adversaries, and the potential specter of climate change threatening basic global stability.

What can Sandia do to help? How can the Labs focus its resources, expertise, and partnerships to best contribute? Sandia's newly created Energy Security Thrust was established specifically to address these questions.

Transcending traditional programmatic boundaries

The objective of this thrust, along with the cyber and nuclear thrusts, says Terry Michalske (6300), leader of the Energy Security Thrust, is to transcend traditional programmatic boundaries by drawing on expertise and capabilities housed across the Labs to best produce solutions to significant, complex, systems-level problems.

"We must take a more systematic approach to focusing our internal capabilities in energy S&T, systems engineering, and security approaches on key energy security challenges," says Terry.

Just as Sandia has provided systems-level solutions for the nuclear weapons enterprise, he says, the Energy Security Thrust will use core capabilities to develop and strengthen the Labs' role in informing the nation's energy security strategy. Drawing on the Labs' achievements in energy-based work, the Energy Security Thrust is uniquely equipped, Terry says, to address systems-level energy security challenges on three main fronts: reducing oil dependence, assuring operational energy, and assessing climate change.

"Each day, the US spends almost $1 billion importing oil from other countries," says Andy McIlroy, senior manager in Chemical Sciences Dept. 8350 at Sandia's Combustion Research Facility. "Our country's vast dependence on fossil fuel makes our economy and national stability increasingly vulnerable."

High prices for fuel, competition for finite resources, increased risk of global climate change, and threats to political stability are some of the dangers posed by a dependence on fossil fuels. To address these challenges, the Energy Security Thrust is developing solutions such as advanced research in combustion efficiency, alternative fuels, and developing safer, more reliable batteries.

The second focus of the Energy Security Thrust is ensuring operational energy. A reliable energy infrastructure is the foundation of any essential operating system. Systems such as military facilities require reliable energy infrastructures to ensure mission readiness. However, energy infrastructure is vulnerable to both physical and cyber attacks.

Providing microgrid technology to military bases

"The past is marked by a lack of coherent energy security and reliability strategy with regard to secure microgrid development in military installations," says Dan Rondeau (5340), program director for Sandia's Homeland Defense/Force Protection. "However, Sandia is actively engaged in providing microgrid technology to military bases, as well as developing and testing other technologies to better integrate alternative energy into mission-critical operating systems."

In the area of ensuring operational energy, Sandia is developing new technologies to improve component and system reliability, advance cost-effective energy storage, and improve cyber secure smart controls.

Climate change assessment is the third focus area of the Energy Security Thrust. Although climate change will affect each part of the world differently, assessing it will help reduce the risk of negative climate impacts on society.

"Sandia is currently developing its complex systems-modeling capability," says John Mitchiner, senior manager in Computational Science R&D Dept. 1430. "Using high-performance computing, we can produce sophisticated physical and societal models of climate impacts to gain insight into this global concern."

Data-gathering and analysis also play prominent roles in the suite of capabilities dedicated to assessing climate change. The Energy Security Thrust promotes collaborative ventures to design monitoring and verification systems and to conduct consequence assessments. Working in close partnership with the National Center for Atmospheric Research, Sandia is poised to actively engage in the global climate change dialogue. Work done at Sandia helps inform policymakers by better equipping them to address issues of global vulnerability mitigation as well as adaption.

Initiating a new approach for energy security mission

As the challenges of energy security continue to rank as high priorities in national security strategy, it is more important than ever, Terry says, for Sandia to initiate a new approach to fulfilling its energy security mission.

Specifically, the Energy Security Thrust will invest in enabling systems science, identifying and mapping customer/ partner networks connecting SMUs, pursuing specific policy issues that Sandia can inform, and implementing a communication strategy engaging both internal and external stakeholders. Combining capabilities, resources, and talent from across the Labs, the Thrust can address energy security challenges more effectively, providing better solutions to our customers, Terry says.

"Connecting Sandia's programs to the Energy Security Strategic Thrust gives us broad positioning to better serve our customers," says Div. 8000 VP Rick Stulen, champion of the Energy Security Thrust. "We will be able to devise appropriate and effective solutions to meet the complex set of energy and climate challenges they face in the coming years."

Energy security at Kirtland AFB

In April, Sandia launched a study to evaluate Kirtland Air Force Base's (KAFB) electric power system. The goal is to develop approaches to improve the base's energy security and reliability using the Sandian-developed Energy Surety Microgrid™ (ESM). ESM is a risk-based methodology enabling the base to use renewable energy resources for environmental benefits while also increasing energy security and reliability and enhancing critical mission assurance.

"The results of this study will allow us to better understand the actual impact of power interruption to Team Kirtland and how we can enhance energy surety for our most critical missions," says Col. Robert Maness, 377th Air Base Wing commander.

Following the assessment, scheduled to be completed by October, Sandia will work with the NNSA Sandia Site Office and the KAFB installation commander to assess technology investments needed to improve the base's operational readiness, enhance mission assurance, and extend the duration of energy system performance.

US Navy

(Continued from page 1)

as navigation policy and standards.

Mixing humor and environmental charts from the Applied Physics Lab at the University of Washington, Titley said the Navy was concerned that ocean levels would rise "a meter or two" over the next century, the result of the accelerating melting of the Greenland ice sheet and continued melting and thinning of Arctic ice.

"Why does the Navy care about this?" he asked. "We tend to build our bases at sea level. It's a Navy thing," he said straight-faced.

Faced with a situation that might require building dykes around its bases, the Navy reacts, he said. Navy oceanography cannot be "just scientifically cool," it must have a practical outcome that transforms information into decisions. Otherwise, Titley said, imitating an impatient interrogator, "Tell me again why you're here?"

REAR ADM. DAVID TITLEY, Oceanographer of the Navy, is seen here on the right in a recent Navy ceremony in Washington. Titley spoke at Sandia about climate change and its potential impact on the Navy. (US Navy photo by John F. Williams)

He said the problems the Navy anticipates over the next century, after engaging nearly 400 people from more than 120 organizations to help gather data, include:

- environmentally forced or opportunistic changes in shipping routes,
- political problems as islands disappear beneath rising seas or ports become lower than sea level,
- increased economic activity in areas currently off-limits because ice at present blocks maritime access, and
- possible negative effects on plankton when the salinity of the ocean changes.

"Where will one billion people who get their protein from the ocean get it when the tiny living beings that form the bottom of their food chain disappear?" he asked.

There was also, he said, "the human dimension that I'm not sure the policy folk always think about: humans want to stay where they are," regardless of the alteration of the environment about them.

He predicted partnership opportunities and new energy security initiatives.

So, he said, he was interested in partnering with the national labs to develop better operational decision-making capabilities with respect to climate change.

Terry Michalske, who leads Sandia's Energy and Security Systems Center 6300, chatted with Titley at some length after the talk. Says Terry, "[Titley] had no doubt that climate change was happening. He was interested in our risk-and-consequence approach that we undertake at places like NISAC [National Infrastructure Simulation and Analysis Center]. We're not worrying about the reasons why the climate is changing, but we accept data that shows it is. So, we need to better understand that change and its impact on society as it may affect us in the immediate future.

"I think there's a piece here that fits Sandia well," he says, "with our links to the intelligence community, our studies of economic trends, and our technical capabilities all applied together to a massive global event. I think Titley was very encouraged by many of the capabilities he learned about at talks while here at Sandia."

Says Rob, "While there are many opinions on the large subject of climate change, we're focused here on the technical and social issues that pertain to national security. The goal is to inform the internal dialogue and seed an understanding more broadly of Sandia's potential contributions."

Titley came away with a better knowledge of Sandia's capabilities, says Rob. "When we briefed him on our risk framework and probabilistic impact approach, he said, 'This is the best stuff I've seen on the subject.' I believe his intent is to build a broad coalition across the government sector to address climate change. He's got high-level military support for that, and we'd like to position Sandia to make a central contribution."

Cybersecurity

(Continued from page 1)

"Adversaries continually develop new attack vectors, new things that could exploit vulnerabilities in the systems that we have. They've gotten quite sophisticated. They're now exploiting the applications that we use."

—Sandia Chief Information Officer Art Hale

Photos by Lloyd Wilson

Having gained a foothold on those machines, the adversaries can plant things that compromise the machine. So when we go there with a simple query, a simple download of a file, not only do our employees get what they went there for, they might get a little something "extra." It bypasses the things that we do to filter and block attacks. It goes right into our machines and compromises them.

Adversaries continually develop new attack vectors, new things that could exploit vulnerabilities in the systems that we have. They've gotten quite sophisticated. They're now exploiting the applications that we use. A common one is the Internet browser, such as Internet Explorer or FireFox or a whole range of others. They all have vulnerabilities that can be exploited.

But also there are other things like Flash, PDF files, Microsoft Word, and PowerPoint and Excel documents. Adding a little extra piece of code to any of those files might enable the attacker to take over a machine once the code gets into our environment. It's not just the viruses that we used to have, which would cause damage to a computer. The current threats I'm mainly concerned about are those that are after information. Our adversaries want a foothold. Once they get it they want to maintain it. They want to exfiltrate information, but sometimes they can do it slowly, and try to expand their presence over time.

Far from helpless

LN: *Are we helpless against members of the work force innocently going out to check a news story or something, and inadvertently bringing in a threat?*

Carol Jones: We're far from helpless. The Cyber Security team works diligently to introduce new processes and tools in order to protect us. As Art mentioned, the adversary is also sophisticated, so they continually increase their methods of entry. But we've developed additional protections. As a recent example, we have implemented a tool called Blue Coat that examines files retrieved through the Internet.

We also monitor our network to look for patterns of behavior that we know are attributable to computers that have been compromised — something unusual or not part of the normal traffic. This monitoring can help us pinpoint computers that have become infected with malicious code. We see two or three times a month on average that a computer becomes compromised. And of course we then clean it up.

Art: We see things come in that could compromise a computer, probably a dozen times a week. We catch a lot of things that could have compromised a machine, because they had some kind of malicious payload.

And then of course there are all the attacks hitting the perimeter. That's on the order of hundreds of thousands a day. Perimeter defenses keep out the unsophisticated attacks.

These are the kind of things that we know about the attacks. Of course, there's always concern about what we don't know.

LN: *What do we do about what we don't know?*

Art: One thing is to deploy a more secure operating system for the majority of our work force, and we're doing that. Windows 7 is much more secure, particularly the 64-bit version. It has a lot of features that use the power of the hardware to check software coming in. It's much harder to attack and exploit that operating system.

So introducing Windows 7 and Internet Explorer 8 is one of the first steps, making that the default operating system for new machines that come into the Labs and any rebuilt machines. We would like to move aggressively from Windows XP to Windows 7. It's a big endeavor because we have so many thousands of computers that are running Windows XP today. At some point in the future, at a date we have not determined, we expect to sunset all legacy operating systems, including XP, or quarantine those that need to continue to exist.

TOM KLITSNER

LN: *Are we handling Windows 7 differently than we did Vista, which also offered increases in security, but hasn't turned out to be widespread throughout Sandia?*

Tom Klitsner: The television commercials are better! I'm half-kidding, but only half. The press on Windows 7 is much better, and people's experience with Windows 7 is much better. The operating system is more friendly, and works better on both old hardware and new hardware. So I think user acceptance is already higher than it was when Vista came out.

Another thing is, we've looked carefully at how to implement security. We've worked with Cyber Security to come up with a compromise that provides high security levels but also high functionality levels within Windows 7.

Getting XP upgraded to Win 7

LN: *So, those thousands of computers running XP — what's it going to take to get them upgraded?*

Tom: As Art says, new computers coming into the Labs, and any that are rebuilt as part of a repair, will by default get Windows 7. For the others, we will convert the systems in a scheduled fashion. We're going to use some new techniques called Zero Touch and Light Touch to migrate systems, hopefully at night, some number each night. Of course we will coordinate with the owners first.

Some users may need XP to run a certain application or have a certain function. We can give them access to a "virtual machine," which they use essentially the same as a computer on their desktop, but which is actually running on a server in the data center. That's one of the options we're looking at.

Art: We've been taking a lot of steps to provide virtual desktop environments. One of our vulnerabilities is that we have so much of our data and our applications out in the end-user devices — user computers and user disk storage. In a future state, that information will be potentially more useful if it's in a data center. We can migrate both the data and the applications, to a significant degree, into data centers. That's the long-term path. It's not going to happen in a year or two. But over a period of multiple years, more and more of what we do will go back into servers in a data center somewhere.

As we start to move our information to the data center, then we start to take more steps to protect the data center. At the same time, we can start to relax the steps, or at least the proliferation of new controls, that we need to put on the devices that the users actually touch.

So we might be able to allow other kinds of devices, like iPads as an example, which have been taking the world by storm in the past few months. Those devices could be part of our work environment to let people do things on a virtual desktop that would be in a data center (see "Bright future for cloud computing," below left).

There's a sequence of changes that will happen as technology evolves and as the needs of the business, the missions, also evolve. We're going to enable a lot of those mission needs and uses of new technology by the way we provide security. Things like Windows 7 and Internet Explorer 8 are just the beginning. There are other things that we have today, such as a pilot program to permit the use of BlackBerry devices inside limited areas. We can do this through security controls that give people more capabilities without adding significant risk.

Convenience vs. security

LN: *Are users going to have to give up convenience for the improvements in security?*

Carol: They may see some changes. One example is that there's a real risk with the current eight-character passwords, the possibility of them being cracked quickly. Going to 16-character passwords would reduce that risk. But our philosophy is to look at the total threat spectrum, all the attack vectors that we're seeing. We haven't yet determined whether the decrease in convenience to the user would be worth the increase in protection of a longer password.

CAROL JONES

Cyber Security is undergoing a reform where we're moving away from compliance with specific oversight rules to a risk-based program. In the next year we'll be taking a hard look at our technical controls and policies. The question is whether those technical controls and policies actually mitigate the risk as intended.

So you may see new controls, but you'll also see an offset in some controls being removed. We're trying to look at the total picture, apply effective safeguards for the actual risks, and keep Sandia's people working securely and productively.

Bright future for cloud computing

During a discussion of cyber threats and upcoming software changes, Art Hale (9600) and Tom Klitsner (9300) also looked into the more distant future — maybe not terribly distant. What is cloud computing, and what might it mean for Sandia?

Tom says, "There's a natural evolution that information technology providers and their users will take. The web has changed the way we do everything in information technology, and will continue to do so. Companies like Google have made the case that the computing model of the future could put your computing capabilities on the web rather than within your own local desktop.

"Over time, that makes sense. Take Sandia's internal web. We wouldn't be able to operate without the applications that run from there — timecard, expense reports, and so on. There's also a lot of advantage to running Office-type applications on the network. Your data and your applications both would reside on the network and would be accessible anywhere you go. If you need to share that information with others, it's more accessible than if it were stored either in your own desktop or in your own network share."

The "cloud," then is basically the Internet, or some part of it, used to provide computing services. It's "cloudy" because (unlike in desktop computing), the user doesn't know exactly where software and data are located. Such an arrangement would work well for collaboration and remote access, says Art: "Probably in the near term we would think of making our internal environment more cloud-like. So we might have a Sandia cloud that would be accessible over the Internet through appropriate protection mechanisms."

But the changes could go deeper, Art continues: "There's an opportunity to rethink how we develop applications. Today, our enterprise applications are designed to do many specific things, but there's not a built-in awareness of who you are, what you want to do, what your patterns of use are, or the tasks or information that you would be interested in. So there are things we can do to improve the productivity and the overall experience of Sandia workers using the internal environment. I like to think about having the capability of the entire laboratory at our workers' fingers, rather than just the capability in the one computer or few computers they have currently at their desks.

"I believe we're limited in our ability to create the future environment because of the way we think about computers and how we interact with them."

Art points out that interacting with computers through the keyboard and mouse was introduced commercially by Xerox in the early 1980s and popularized a few years later when Apple introduced the Macintosh. "So our mode of interacting with computers has been the same for several decades," says Art. "Cloud computing is an opportunity to completely change that. You could have a window into an environment, perhaps a simple tablet, something like the iPad. It wouldn't need to store a lot of information if it's always connected wirelessly into this greater power of computing all over the world. It wouldn't need to have as much capability embedded in it. There's a whole new set of things that people will start to create, using the power of cloud computing. It's going to take time to see how they develop."

Art offers a challenge: "We have a lot of creative people at Sandia, talented people who can envision a whole set of things that are far beyond my ability to envision. We need to unleash their creativity and innovation to do these things on behalf of the missions of the Laboratories."

— Charles Shirley

PeopleSoft

(Continued from page 1)

Time charging increments in PS v9.0

TRC	Time Charging Increment		
	Exempt Employees	Non-Exempt Employees	Represented Employees
241 – Vacation 251 – Sickness 261 – Exam at Medical 271 – Personal Absence ILL	1 hour	15 minutes	Refer to contract
288 – Flex	1 hour	N/A	N/A
290 (as well as 291, 292, 294, 295, 299) – Corporate-wide Mandatory Training	30 minutes	15 minutes	Refer to contract
PTO	N/A	N/A	Refer to contract
All other TRCs	Refer to the applicable Corporate Policy.		

been provided through previous *Lab News* articles, the upgrade website, and the toolkit, this article provides an overview of some of the key changes that will be implemented in the move to PeopleSoft v9.0. Additional information regarding the upgrade or how system functionality will change can be found at the upgrade website, http://upgrade.sandia.gov.

Why upgrade?

The preceding PeopleSoft system was highly customized by Sandia to meet business process needs. These customizations made upgrades difficult and created an inherently unstable system. It also introduced other bugs into delivered PeopleSoft security updates.

A small number of applications previously separate from the human resources information system will be moved into the PeopleSoft v9.0 system and share a common look and feel. For example, the timekeeping system, Spot Awards, Employee Contribution Program, and Savings Bonds will all be part of the upgraded PeopleSoft. Overall, this will result in fewer costs to the Labs in supporting PeopleSoft and its functions.

Impacts of the upgrade

Several areas of PeopleSoft that members of the workforce routinely interact with will be affected by the upgrade. These range from areas associated with benefits, manager self-service, payroll, and compensation, to recruiting and time reporting processes.

Downtime

The current version of PeopleSoft will be brought down Friday, June 18, for the upgrade to PeopleSoft v9.0. PeopleSoft will not be available from Friday, June 18, to Sunday, June 20. Enterprise Person and Web Services (i.e., Foreign National Requests, Access Control Enabling System, WebCARS) will also not be available during this time.

Time reporting

With the release of PeopleSoft v9.0, Sandia's Electronic Timekeeping application (ETK) will be replaced by a new timekeeping application, Time and Labor (T&L). The on-line Electronic Timekeeping Course (ETC100) was updated to reflect the new application, and was released in May. This is a mandatory training course assigned through TEDS. The current time invoice system for contract associates will remain in place.

Beginning the week of June 24, employees' timesheets must be entered by 6:30 p.m. MDT each Thursday. The deadline for managers to review and approve the timesheets will be 7 p.m. MDT on Thursdays. Nonexempt employees who do not submit their timesheets by the Thursday deadline will be at risk of not receiving timely pay.

In cases where an employee has submitted a timesheet and his or her manager has not approved it, the submitted timesheet will be processed and the employee will be paid for regular and overtime pay.

Time charging

Time charging increments will change with the release of PeopleSoft v9.0. Exempt employees will charge time reporting codes (TRCs) in one-hour increments; nonrepresented, nonexempt employees will charge in 15-minute increments; training TRCs may be charged in 30-minute increments; Flex time will be available in one-hour increments. Represented employees should charge time per collective bargaining agreements.

The T&L application will use time reporting codes instead of A-Orders. This is just a change in terminology; TRCs will serve the same function as A-Orders have previously.

Corrections

After the implementation of PeopleSoft v9.0, employees will not be able to electronically correct timecards that were previously submitted in ETK. The process will be similar to fiscal year-end activity; no corrections can be processed through timekeeping. If there are uncorrected errors on a timecard submitted in ETK prior to Monday, June 21, Payroll will only accept paper timecards for corrections of the weeks ending May 27, June 3, June 10, and June 17.

In the new T&L application, employees will only be able to correct timesheets up to four weeks prior to the current week. If a timesheet is corrected, both the employee and manager will be sent an email confirmation that the change was made.

Work schedules

In most cases, work schedules (standard or 9/80) will automatically transfer from the old ETK application to the new T&L application. However, prior to submitting a timesheet for the week of June 18-24, employees should verify their work schedules are correct.

ACTION ITEM

Prior to submitting a timesheet for the week ending Thursday, June 24, in PeopleSoft's new T&L application, all employees should verify their work schedule has properly transferred from the old ETK application. To do this, open your timesheet and verify the schedule listed next to "Scheduled Hours" is correct. If it is not correct, contact the Payroll Helpline at 844-2848. After the week ending Thursday, June 24, employees can change their schedule through HR Self-Service.

Time allocation

Time allocation previously existed as an optional time-charging process available to department managers, team supervisors, and authorized office assistants and staff members. This feature enabled these individuals to have the timecard application automatically divide up or allocate projects and tasks based on the time charges submitted for a work week.

Time allocation will be discontinued with the implementation of PeopleSoft v9.0. Every employee is expected to charge his or her time to the appropriate project and task. Simply stated, everyone should charge work directly to the benefiting project.

For additional guidance regarding time allocation, see the Payroll homepage.

Extended work week

The extended work week (EWW) — when straight time hourly pay is more than 40 hours in a week for exempt employees — will require a vice president's approval, which is to be obtained by an employee's manager. Time charged to the EWW time code then requires weekly approval by the employee's manager, and will not be compensated unless this approval is received.

ACTION ITEM

Beginning the timecard for the week of Friday, June 18, to Thursday, June 24, employees who are currently approved for EWW will begin charging time in excess of 40 hours to the EWW time code. Managers must approve any time charged to the EWW time code by 7 p.m. on Thursday of each week for the employee to receive EWW pay.

Vacation

New-hire employees will receive a vacation balance immediately if they are on-roll as of a pay period end date. Additionally, accrued vacation will now be credited to employees' vacation balances twice monthly, instead of once monthly.

upgrade
Training and Help

June 2010 → Training and help is available for the launch of PeopleSoft v9.0. Refer to upgrade.sandia.gov for a complete listing of demos and training material.

http://upgrade.sandia.gov

Employees who participate in the Vacation Buy program will no longer have to exhaust all available balances in their Vacation and Flex accruals before using their bought vacation.

Administrator of record

With the implementation of the upgrade the secretary of record will become known as administrator of record (AOR). In PeopleSoft v9.0, AORs may view, correct, and submit timesheets for employees in their organization. AORs must be employees or staff augmentation contractors in the following categories: office administrative assistants, office management assistants, senior management assistants, limited-term employee Office Professional Employees International Union-equivalents, and executive assistants.

ACTION ITEM

For organizations with an AOR not in one of the above categories, the manager will need to update the assignment on Monday, June 21, through a link under Manager Self-Service.

Delegation

Delegation of Personnel Actions and Enterprise Person actions will now be done in PeopleSoft (through Manager Self-Service) rather than through Roles and Delegations of Authority (RDA).

ACTION ITEM

Current delegations for EP will be automatically brought forward into PeopleSoft. Current delegations for PA approval will not be brought forward, and must be re-entered in PeopleSoft v9.0 on or after Monday, June 21.

Those who are delegated PA and EP actions in PeopleSoft will receive an email requesting their consent. They must accept the delegation in order for it to take effect.

Unified hire process

Requisitions will now flow internal and external applicants into a single, unified hiring process. Where the activities have been markedly divergent in the past (separate processes and postings), internal and external applicants will now bid and be dispositioned on the same posting. Managers will still have the flexibility to only post an opening internally.

All active Sandia employees, including student interns, LTEs, post-docs, recurrent, and faculty sabbatical employees will now be able to bid on internal postings.

Self-service

PeopleSoft v9.0 will allow employees to electronically input their own direct deposit information through HR Self-Service. Paychecks and advice statements will also be available in PDF format for employees to view and print at any time.

Transition assistance

If you have general questions about the upgrade prior to the launch, contact the project team at wg-upgrade@sandia.gov. Following the upgrade, questions regarding the new PeopleSoft system's functionality can be directed to the Corporate Computing Help Desk (845-CCHD) by choosing option "0" (zero).

Payroll- and timecard-specific policy or process questions should continue to go to the Payroll helpline at 505-844-2848. Benefits-specific policy or process questions should continue to go to the HBE Customer Service line at 505-844-4237. If you have any questions regarding hiring or applying for jobs, contact your division staffing partner.

Anything but routine

Sandia team honored by NASA for developing on-the-fly workaround in wake of shuttle *Discovery* antenna glitch

Note: Ever since the NASA space shuttle fleet returned to flight in 2005 after the 2003 Columbia *accident, Sandia has been a key member of a team that helps ensure the integrity of the all-important thermal protection system (TPS) — the heat-absorbing tiles that protect the shuttle during re-entry. It was that system that was breached during the* Columbia *launch and subsequently failed during re-entry. In a recent mission — STS-131 — the failure of a key antenna on the shuttle* Discovery *meant that the data used by the Sandia/NASA team to evaluate the TPS was going to be very difficult to get from the spacecraft to the ground for analysis. The Sandia team members and their NASA colleagues scrambled for a solution, ultimately developing an approach that got the job done with time to spare.*

In this first-person account, written at the request of the Lab News, *Sandia project lead Jose Rodriguez conveys a you-are-there sense of urgency to work the problem and help ensure the astronauts got home safely. The team was honored by NASA mission planners for its efforts.*

By Jose Rodriguez (2664)

In the early morning hours of April 5, my cell phone alarm went off. It was 4 a.m. Of course, like most people do, I hit the snooze button trying to squeeze in that little bit of extra sleep. When the alarm went off again five minutes later, I decided it was time to get up. The space shuttle *Discovery* was launching in 15 minutes and I had to see it. Over the past several years, I've watched almost every shuttle launch and I wasn't about to miss this one. My job depends on it.

I am the project lead for the Sandia LOIS team. LOIS, by the way, is the LDRI Orbiter Inspection System. LDRI stands for laser dynamic range imager. We use a lot of acronyms in this business, but you get used to them. Our LOIS team has been an integral part of the space shuttle program ever since the Return to Flight mission following the *Columbia* accident.

Let me give you a little bit of background: You may recall that what destroyed the *Columbia* was the damage to its thermal protection system — the TPS — when a chunk of foam insulation broke away from the spacecraft's main fuel tank during launch and slammed into the orbiter wing's leading edge at supersonic speeds. The damage compromised the spacecraft's protective skin, allowing the massive heat of re-entry to burn its way into the shuttle's structural framework. *Columbia* broke up over the southwestern US; pieces were recovered in Texas and Louisiana. All seven members of the crew were killed.

The fact is, the *Columbia* was doomed from the moment that insulation damaged the TPS, but the astronauts on board and controllers on the ground had no way of knowing that — and no way to repair the craft, if they had known.

This is where Sandia comes in. We designed and built the LDRI to inspect the TPS to check for any damage due to ascent or orbital debris. LDRI provides high quality 2-D and 3-D video, enabling us to see damage that a regular video camera might not detect. Using our system, the astronauts can scan the spacecraft while in orbit. We work with NASA at Houston's Johnson Space Center (JSC) during shuttle flights to process and analyze LDRI data. We generally report to JSC within a few hours of a successful launch to begin that process. In the event an LDRI scan *does* reveal any TPS damage, NASA has put a number of contingency plans in place to ensure the safety of the crew.

As I jumped out of bed on April 5, our LOIS team had completed 17 successful missions and number 18 — shuttle mission STS-131 — wasn't expected to be any different. I flipped open my laptop and logged onto spaceflightnow.com to watch the launch. All systems were "go" and space shuttle *Discovery* blazed into orbit in what would probably be the last night launch of the space shuttle program. (The shuttle fleet is scheduled to be retired this year.) I really wish I could have been there to view it, but I had to head to the airport and catch the next flight for Houston. I had to be at the JSC for my shift, scheduled to start at 9 p.m.

NIGHT MOVES — Space Shuttle *Discovery* launches from Launch Pad 39A on April 5 in a spectacular night launch. STS-131 marks the 35th, and possibly last, night launch of the space shuttle. The space shuttle program is scheduled for retirement at the end of 2010.

KU antenna down

My plane landed in Houston at around 9 a.m. When I turned on my cell phone there was a voicemail from one of my NASA coworkers, Dan Smith. The KU antenna, he said, was not working and probably wouldn't work for the rest of the mission.

Oh, great, I thought. The KU antenna is the high-bandwidth communications and data downlink for the space shuttle. It provides the highest-fidelity downlink for getting LDRI data to the ground. All of a sudden STS-131 wasn't going to be a routine mission, after all; this flight was going to be a challenge for everyone on the team.

I grabbed my luggage from baggage claim, picked up my rental car, and drove directly to the JSC. I would have to check into the hotel later.

Dan Talbert (5711), who maintains our Sandia presence from beginning to end during shuttle missions, was coordinating with our NASA coworkers when I arrived at JSC. The NASA team was already working on a solution to get the LDRI data down to the ground. I have to credit them with how quickly they tackle problems that arise during missions. They had a couple of workarounds in hand, and I advised them on the pros and cons of each from the LOIS ground station perspective.

We had two big concerns: We wanted to minimize the loss of data quality and we wanted to get the data to the ground as quickly as possible.

One idea, the obvious one, was to use the International Space Station's (ISS) analog downlink. It was a feasible solution, but not our best option. The data quality would most likely be severely reduced in comparison to our normal data downlink. Another solution was to have the astronauts create AVI files — that's a common video file format — from the LDRI data using Windows Movie Maker and then transfer those AVI files to the ground from the ISS. The idea was that the AVI files would have a lossless transfer to the ground in comparison to the other options that might throw away LDRI data. Essentially, it would be like downloading a movie from the Internet. This solution, while it sounded promising, made me a bit nervous: Windows Movie Maker, which is bundled with the Microsoft Windows operating system, was untested for this purpose. We didn't know how it would treat the LDRI data and this was a heck of a time to find out.

MEMBERS OF THE LOIS TEAM discuss the various options for downlinking the LDRI video at mission control. Standing in picture are Bob Nellums (5711, left) and Jose Rodriguez (2664, project lead). Seated in the photo are Brenna Hautzenroeder (2623) and Todd Pitts (5711). Out of focus in foreground is Jim Heslin of NASA. (All photos courtesy of NASA)

Since we were going into new territory here, I decided it was time to call all our team members together to help out with the analysis. Would the AVI solution work? Was it viable? The call went something like this, "Hey, it's Jose. KU antenna is broken. Early inspection will proceed as normal. Need to evaluate proposed downlink methods. If you're in Houston, come into MCC. If you're still in Albuquerque, get to Houston, as quickly as possible."

As the full LOIS team assembled, we analyzed each option. To my pleasant surprise, our analysis convincingly showed that the Windows Movie Maker solution worked fine. We determined there would be zero loss in data quality compared to our normal data downlink. There were huge smiles on everyone who was helping out with the analysis. It was 7 p.m. by now, just three hours before the scheduled first LDRI inspection of the space shuttle.

A huge challenge ahead

NASA controllers filled the crew in on the workaround and briefed them on the revised procedure: In addition to the nominal LDRI scan, the *Discovery* crew would need to convert the collected data into AVI files.

The early inspection of the space shuttle proceeded as usual and the crew reported that recording of AVI files was completed successfully. We didn't have any other hiccups during the inspection, which was an added relief because we already had a huge challenge ahead of us

(Continued on next page)

Sandia to play major role in simulation of 'virtual' nuclear reactor

By Neal Singer

Sandia computational scientists will lead two of five technical areas in a DOE effort to create a "virtual" nuclear reactor, to be headquartered at Oak Ridge National Laboratory (ORNL).

The advanced simulator will use capabilities of the world's most powerful computers to attempt significant leaps forward in nuclear reactor design, engineering, and operation. Information gleaned from a virtual model of a currently operating reactor could help improve nuclear reactor safety, increase reactor power production, and extend reactor life and licenses over the near, mid, and long term.

The work, funded by a DOE award of up to $122 million over five years, will be coordinated from a Nuclear Energy Modeling and Simulation Energy Innovation Hub at ORNL.

The Hub, named the Consortium for Advanced Simulation of Light Water Reactors (CASL), includes partners from universities, industry, and other national laboratories. CASL is tasked with delivering computer models that simulate nuclear power plant operations. These models would then be incorporated into a computational environment that forms a "virtual reactor" for the predictive simulation of light water reactors (LWRs).

"Sandia fully supports the exceptionally strong CASL team assembled by ORNL," says Steve Rottler (1000), Sandia's Chief Technology Officer and VP for Science and Technology. "Accomplishing the CASL vision is vital to the expansion of nuclear power and long-term energy security for our nation. I have full confidence that we can achieve our ambitious goals."

Sandia scientists and engineers will provide technical leadership and expertise in two of the five technical focus areas of the hub: Virtual Reactor Integration (VRI) and Verification, Validation, and Uncertainty Quantification (VUQ).

VRI focuses on the integration of computational models that will form the heart of the virtual reactor. "Accomplishing our mission will have an enormous impact in support of nuclear energy in this country, and I am thrilled to be part of it," says Randy Summers (1433), manager of Sandia's Exploratory Simulation Technologies Department and co-lead of the VRI focus area that includes scientists from ORNL and Idaho National Laboratory (INL).

Sandia scientists will also team with researchers from North Carolina State University (NCSU) to incorporate advanced methods for verification and validation of the computational models and for quantification of their uncertainties as they are executed within the virtual reactor. Analyses using more tightly coupled models, with better-understood uncertainties, could support license applications for increased plant power levels, improved fuel burn-up and extended plant lifetimes.

"This Hub has the ability to transform the nuclear power industry through the research, development, and application of new mathematical models, advanced computational methods, and leading-edge high performance computing," says Jim Stewart (1411), manager of Sandia's Optimization and Uncertainty Quantification Department and lead for the VUQ focus area within CASL. "Accomplishing Hub goals will require outstanding scientists to work together like never before possible. The CASL team has the broad background and experiences necessary to take on this exciting challenge."

Other institutional members of the CASL team are the Electric Power Research Institute (EPRI), Palo Alto, Calif.; Los Alamos National Laboratory; Massachusetts Institute of Technology, Cambridge, Mass.; Tennessee Valley Authority, Knoxville, Tenn.; University of Michigan, Ann Arbor, Mich.; Westinghouse Electric Company, Pittsburgh.

DOE recently announced that the Hub will be funded at up to $22 million this fiscal year and then at an estimated $25 million per year for the next four years, subject to congressional appropriations. More information on the hubs can be found at: http://www.energy.gov/hubs/

Shuttle

(Continued from preceding page)

managing the downlink process through the ISS.

Around 3 a.m., with the *Discovery* crew in the middle of the LDRI scan, I left John Sandusky (5711) and Dave Karelitz (9326) in charge at JSC. Brenna Hautzenroeder (2623), Bob Nellums (5711), Todd Pitts (5711), Dan Talbert (5711), and I headed to the hotel for some much needed rest. It had been an exhausting day and I had to be back at Mission Control at 10 a.m. to meet with the NASA mission evaluation team. At the meeting, I passed along the LOIS team's recommendation that we proceed with the AVI file downlink process as the best way to get the LDRI data in hand the quickest way possible. Everyone signed on to the proposal. We were good to go; the data download would start the next day at 5:30 a.m. after the shuttle had docked at the ISS.

By now, we were already a day behind our normal schedule, but there was nothing normal about our small but vital piece of this mission. Everyone on the LOIS team was eager to get their hands on the data so it could be processed and analyzed for shuttle damage.

Things finally beginning to click

Expecting the data download to start at around 5:30 a.m., I headed into mission control an hour or so early. Unfortunately, the first AVI file with useful data wasn't downloaded until around 9:30 a.m. That file contained the LDRI calibration data and the first few scans of the starboard wing. Things were finally beginning to click. We were happy that we could start processing and delivering our data over to the NASA screeners.

Our happiness was short-lived, though — the next AVI file didn't get downloaded until five hours later. The next 18 hours went on like this: We would get an AVI file, process it, and then wait four or five hours for the next file.

ASTRONAUTS Dorothy Metcalf-Lindenburger (NASA), Naoko Yamazaki (Japan Aerospace Exploration Agency, JAXA), Stephanie Wilson (NASA), and Tracy Caldwell Dyson (NASA) take part in a quick photo opportunity. STS-131 marked the first time that four women have been in space at one time.

Needless to say, it was very frustrating. It turns out that the file size (6-7 GB per file) was a little large for the space station's network. Also, the predicted data rates weren't being achieved and file transfers would fail due to loss of satellite coverage. NASA's Comm and Track team was handling the file downloads for us and I have to credit them with how diligently they worked to get the data to the ground. I know it was frustrating for us because we were data-starved, but I'm sure they were feeling the pressure, too, to get the data down as quickly as possible.

PHONE HOME — Todd Pitts (5711, foreground) takes a break from mission control activities to call home. The LOIS team worked long hours over many days due to the KU antennae not working. In the background are Bob Nellums (5711, standing) and Shawn Ward (NASA).

Ultimately, it took just over 24 hours to download the AVI files and additional four hours to complete the processing, for a total of 28 hours. In comparison, we usually take about 19 hours to download, process, and deliver our data to the NASA screeners for the early inspection of the TPS.

We all pulled long hours during this process; I stayed for 22 of those 28 hours, which is the longest shift I've spent since being part of the LOIS team.

After reviewing our data, the NASA screeners cleared *Discovery* for tentative re-entry ("tentative" because there is always a potential for damage to the TPS due to micrometeorite impacts, which have happened in the past. A late inspection right before re-entry looks for any damage that might have been incurred while the spacecraft was in orbit.)

A big push for speed-up

Speaking of that late inspection, I spent the next couple of days attending meetings with NASA personnel to discuss how to improve the time-consuming download process. There was a big push for this speed-up because the space shuttle needs to be fully cleared for re-entry before a certain point in the mission timeline. If it isn't cleared, the shuttle needs to go back to the ISS for safe haven.

Fortunately, we developed a simple plan to just use smaller files for the late inspection so that file transfers would be more frequent and put less stress on the ISS network. With the plan in place, I headed back to Albuquerque for a quick couple of days off. It was April 10; the last five days had been fairly intense.

April 16, the date for the late inspection, came quickly, and as the LDRI data came streaming in via those smaller AVI files, we found that our improved download plan was working out great. We received the entire data set in less than eight hours and had processed and delivered the data to the NASA screeners in about 18 hours from the start of the late inspection, which is what we usually average. The screeners cleared the TPS for re-entry and NASA set *Discovery's* re-entry and landing for April 19.

Honored

On April 17, our NASA colleagues informed me that the Sandia LOIS team, along with the NASA Comm and Track team, were being honored by the Mission Evaluation Room (MER) managers for STS-131. We were invited to be part of the STS-131 plaque-hanging ceremony — a tremendous honor and a NASA tradition — for our outstanding contributions during the mission. I was as proud of our team at that moment as I've ever been. It was gratifying to me personally that our long hours and hard work had paid off and was recognized and in its own way contributed to the overall mission success.

On April 20, after being delayed by weather for a day, *Discovery* landed back where it had begun its mission, at Kennedy Space Center in Florida. It was the longest flight in *Discovery's* 26 years of service and 38 missions. On that day, on behalf of the entire LOIS team, I helped hang the STS-131 mission plaque in the MER conference room, which is right across the hall from the old Apollo mission control room. What a way to cap off such a challenging mission.

Sandia-LOIS Team Members for STS-131: Simon Hathaway (2623), Brenna Hautzenroeder (2623), Dave Karelitz (9326), Bob Nellums (5711), Todd Pitts (5711), Jose Rodriguez (2664), John Sandusky (5711), and Dan Talbert (5711).

MISSION SUCCESS — Jose Rodriguez (2664) and Andy Romero (NASA) hang the STS-131 plaque in the Mission Evaluation Room (MER). The LOIS team and the Comm and Track team were both honored by the MER managers for their outstanding contributions during STS-131.

Take Charge Corner

What is an out-of-pocket maximum and how does it work?

Note: This information is provided by Sandia's Benefits organization. Previous Take Charge Corner articles have addressed other "floors" and features of the Total Health house.

This article completes our tour of the Sandia Total Health house. In the four previous articles we took a close look at biometric screenings and health assessments, health reimbursement accounts, preventive care, and the deductible and coinsurance. We learned how the Sandia Total Health plan design shelters the members from excessive healthcare costs. And, as with any solid structure, most shelter is provided by the roof or ceiling. In the case of Sandia Total Health, that shelter for members comes in the form of the out-of-pocket maximum.

The out-of-pocket maximum is the maximum amount you'll pay out of your own pocket for **in-network eligible** medical care during a plan year, including your annual deductible amount. That means any money you pay for **in-network eligible expenses** to meet the deductible also counts toward your out-of-pocket maximum.

The **in-network** out-of-pocket maximum is based on the coverage tier you elect. For Sandia Total Health, if you have:

- Employee-only coverage: your out-of-pocket maximum is $2,750 per year
- Employee + Spouse or Child(ren) coverage: your out-of-pocket maximum is $5,500 per year ($2,750 per person)
- Employee + Spouse and Child(ren) coverage: your out-of-pocket maximum is $8,250 per year ($2,750 per person)

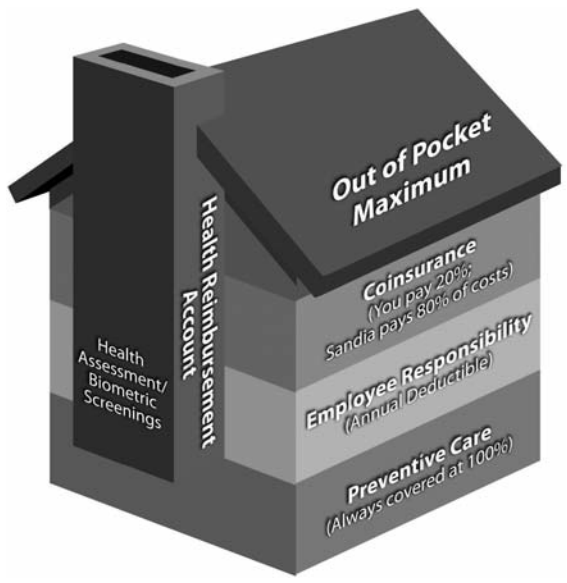
Note: These out-of-pocket maximums apply only to in-network care. Out-of-network care has different out-of-pocket maximums. For more information, review your plan comparison chart.

Once you reach the maximum, your remaining **in-network** eligible expenses for that plan year are covered at 100 percent.

For more information about the Sandia Total Health plan design features, visit the Take Charge website at www.SandiaTakeCharge.com.

The chart below offers an example of how the out-of-pocket maximum works for employee-only coverage.

Remember: If you have more than one person under your coverage, the out-of-pocket maximum will work like this for each individual person under the coverage (up to three times the individual maximum).



Meet Bob: Bob (see chart) has employee-only coverage under Sandia Total Health, and used only in-network providers during the year. Bob completed a biometric screening and a health assessment, so Sandia contributed $250 to his Health Reimbursement Account (HRA). Let's take a look at how Bob's annual medical services are covered by Sandia Total Health.

Important facts about the out-of-pocket maximum:

- **If you have Employee + Spouse and/or Child(ren) coverage, each person covered under the plan has an individual out-of-pocket maximum. That means that when one person meets his/her $2,750 maximum, the remaining eligible expenses in that plan year for that individual are covered at 100%.**
- **Prescription drug costs are not included in the annual out-of-pocket maximum amounts listed above. There is a separate annual out-of-pocket maximum amount you pay for prescription drugs: $1,500 per person for prescription drugs purchased in-network.**

Service	Cost of Service	Description	Claims Processing Amount	Sandia's Responsibility	Bob's Responsibility	Bob's Out-of-Pocket Accumulator
Annual Routine Physical Exam	**$250**	**In-Network Preventive Care Covered at 100% (includes annual well exam)**	**N/A**	**$250**	**$0**	**$0**
Specialist Visit	**$250**	**Health Reimbursement Account (HRA) – $250*** • The first $250 of Bob's eligible expenses is reimbursed by HRA funds, yet still applies toward Bob's deductible and out-of-pocket maximum	**Entire $250 applies to deductible but is reimbursed by HRA**	**$0**	**$250****	**$250****
X-rays	**$500**	**In-Network Deductible – $750** • First $750 of eligible expenses is subject to the deductible • $250 paid by the HRA; Bob pays the remaining $500 to satisfy the deductible	**Entire $500 applies to deductible**	**$0**	**$500**	**$750**
PCP visit	**$100**	**In-Network Coinsurance – You pay 20%, up to $2,000** • Coinsurance applies because the annual deductible of $750 has been met	**20% coinsurance**	**$80**	**$20**	**$770**
Ambulance	**$800**		**20% coinsurance**	**$640**	**$160**	**$930**
Hospital Stay	**$15,000**	**In-Network Out-of-Pocket Maximum – $2,750** • Balance of eligible expenses is covered at 100% for the remainder of the calendar year (not including prescription drugs)	**20% coinsurance**	**$13,180**	**$1,820**	**$2,750** (includes deductible and coinsurance, but not prescription drugs)
TOTAL	**$16,900**			**$14,150**	**$2,750****	**$2,750****

* Annual HRA contribution amounts are $250, $500, or $750, depending on your coverage tier.

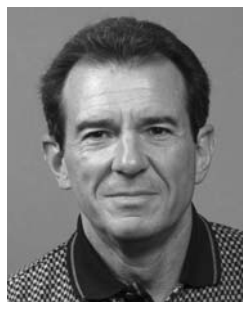
** First $250 of Bob's eligible expenses is reimbursed by HRA funds, yet still applies toward Bob's deductible and out-of-pocket maximum. Bob's actual out-of-pocket amount is therefore $2,500: $2,750–$250 reimbursement from the HRA.

Mileposts

New Mexico photos by Michelle Fleming

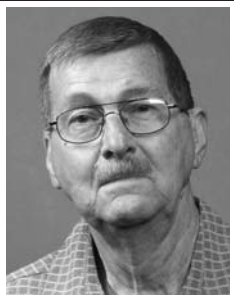

Jeana Brosseau
30 11000


Charles Craft
30 5923


Joe Schofield
30 9535


Graham Yelton
30 1725

Recent Retirees


David Huskisson
39 2555


Cynthia Caton
25 9343

Harry Caton
25 2113


Douglas Doerfler
25 1422


John Fellows
25 5337


Michael Levenhagen
25 1422


Bruce Tuttle
29 1816


Dennis Lierz
25 5335


Fred Oppel
25 6385


Michael Partridge
25 2627


John Torczynski
25 1513


James Cates
20 12311


M. Wayne Davis
20 1100


Kathryn Fortune
20 10541


Brian Geery
20 2113

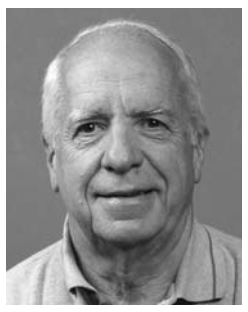

Barbara Jennings
20 9531


Emily Lujan
20 10659


John Parmeter
20 6418


Kent Robbins
20 2542


Patsy Rowland
20 4825


Everett Saverino
20 12320


Martha Bertsch
15 10507


Charles Brady
15 5339


Richard Field
15 1526


Michelle Griffith
15 5578


Marcey Hoover
15 12141


Charles Rhykerd
15 6418


Lisa Trainor
15 5096

Feedback

PeopleSoft questions answered

Q: *Will the Description field, where each individual can enter his/her own text description for each P/T, continue to be available for timecards in the PeopleSoft 9.0?*

A: Individuals are not allowed to enter their own text description for each project and task and were not able to do so in the current system, ETK, either. The project and task that the employee enters is flowing directly from Oracle Financials and is not configurable for any other options in the new timekeeping system. There is a drop-down menu in the new system where allowable project and task data is viewable, but no description for them is identified through the Oracle Financials into the timekeeping module. For further questions/concerns regarding this question, please contact the payroll helpline at 844-2848.

— Donna Kao (10502)

* * *

Q: *For represented: How do we account for including our break times with our lunches? What about the little things like coming in 15 minutes early to leave 15 minutes early for an appointment, etc.?*

A: The new timekeeping system is not a punch clock. The start and stop times are designed to assist in identifying the proper overtime charges for our nonexempt staff. Please refer to your appropriate CPS regarding the inclusion of allowable breaks within a workday. Lunches, as unpaid time, would be recorded during the course of the day. For coming in early or staying late, please work with your manager regarding your schedule. Please also refer to the ETC100 class or call the payroll helpline at 844-2848 for further questions/clarifications. If your questions are related to the HR requirements for breaks, please call your HR representative for that guidance.

— Donna Kao (10502)

* * *

Q: *In the new timecard system is there a way to set up a Project/Task List similar to the old system?*

A: Through the new timekeeping system training, ETC100, we identified that employees will not be able to set up a profile, as they did in the current system, ETK. What the employee *will* be able to do is that after the system is up and live, the employee will be able to go back up to four prior timecard weeks and pull in the project/task setup for a prior timecard week. This will be helpful for employees that are entering similar, multiple project and task charges week to week. For more clarification or other questions regarding this issue, please contact the payroll helpline at 844-2848. *—Donna Kao (10502)*

* * *

Q: *My question is how is this timekeeping change going to affect MOWs' ability to take advantage of the exercise classes offered by HBE at lunch time? Some of the classes are 45 minutes long and it is a wonderful benefit that Sandia has provided to the MOWs.*

A: The timekeeping system has not changed with respect to taking classes offered by HBE during lunch time. Please work with your manager on time charging for attending classes during regular work days. The timekeeping system isn't a punch clock, it is merely being used to assist in determining proper charging for overtime considerations for our nonexempt workforce.

— Donna Kao (10502)

Sandian Sid Gutierrez named 2010 Notable New Mexican

By Stephanie Hobby

A NOTABLE MAN — Sid Gutierrez reacts to seeing the bulto in his honor at the 2010 Notable New Mexican Gala on June 2. Artist Arthur Lopez is second from right. (Photo by Jean-Paul Jager)

Sidney Gutierrez (4100), former NASA astronaut, retired US Air Force colonel and current director of Environment, Safety, and Health and Emergency Management, was named the 2010 Notable New Mexican by the Albuquerque Museum Foundation. He was honored June 2 at the 10th annual award ceremony, where award-winning santero artist Arthur López unveiled a bulto depicting Sid and the story of his life. A bulto is a three-dimensional traditional New Mexican genre of wood carving.

"This is way beyond my wildest expectations," Sid said as the bulto was unveiled. "It really takes my breath away, and I hope that young people who come to the museum will be encouraged to learn and explore more."

The Notable New Mexican award was started as a way to preserve the state's history and to enhance the museum's art collection. Every year, the Foundation recognizes an outstanding individual with unique accomplishments and strong ties to the state. Recipients are presented with a commissioned artwork, which is then permanently displayed at the Albuquerque Museum.

"We are so pleased to present this award to such an inspirational figure in the community," says Debra Romero, executive director of the Albuquerque Museum Foundation. "Sid's life mirrors the history of Albuquerque, from having roots in agriculture to being a central part of the nation's high-tech industry. We see the opportunity to celebrate Sid as an opportunity to celebrate Albuquerque."

Sid's family heritage can be traced back through 300 years of Duke City history, but his family originally descended from people living in the area more than 30,000 years ago.

"My family and I are very excited about the art and this award," says Sid. "I look at this as what it means to my family and my friends. I look back at my ancestors, and my grandfathers in particular, and what they did to get me to where I am today. I look at my teachers who helped me out. I look at my family and friends who supported me, and I have been so fortunate in that regard. This is a great honor, and I am pleased to share it with those who have supported me over the years."

Sid was born in 1951, just four years after Chuck Yeager tore through the sound barrier, and six years before a beach-ball sized satellite named Sputnik changed the world. He grew up on the same North Valley property where his great-grandfather had farmed and raised sheep and cattle.

Like most children who grew up in the height of the US-Soviet space race, Sid was caught up in the fever of space flight and exploring the unknown. He made a commitment to become an astronaut while in fifth grade at Los Ranchos Elementary School. While his peers only dreamed of flying in space, Sid pursued his goal with fierce determination. He contacted NASA to learn the requirements of the astronaut training program and methodically made his way through the rigorous criteria.

SID GUTIERREZ

Sid was accepted to the US Air Force Academy in 1969, the same year that two American men left the first footprints on the moon. Sid studied aeronautical engineering and was a member of the National Collegiate Championship Parachute team. He did more than 550 jumps, and rose to the ranks of master parachutist. Not surprisingly, Sid's perseverance led him to graduate at the top of his class. He became a fighter pilot and then a test pilot before being selected by NASA for astronaut training in 1984. On his first trip to space in 1991, he served as the pilot for the space shuttle *Columbia*, and in 1994 was the commander of the space shuttle *Endeavor*.

Five months after touching down at Edwards Air Force Base, Sid and his family returned to Albuquerque, where he started work at Sandia. He is currently the director of Environment, Safety, and Health and Emergency Management at Sandia.

"Sid is a great New Mexican and a great patriot," says Executive VP and Chief Operating Officer Al Romig. "I can think of few others who have done as much in their lifetimes to make this country great. Sid is surely deserving of this award."

Every year for the past 10 years, the Albuquerque Museum Foundation has presented the Notable New Mexican award to celebrate the accomplishments of an extraordinary New Mexican with strong ties to the state and exemplary service to the public good.

All past award recipients have been presented with a portrait, which is permanently displayed at the Albuquerque Museum. This year, Sid chose to be depicted in a bulto, to reflect his family's New Mexican heritage. The santero artist, Arthur López, is a native of Santa Fe, and has received numerous awards for his work and exhibits his art at shows throughout the Southwest.

A Notable Family Day event, "The Astronaut and the Artist: Storytelling, Inspiration and Craft" will take place July 10, 1-3 p.m., at the Albuquerque Museum and include presentations from Sid and López. This program is free to the public.

Talented group helps bring talent into Labs

ORDER OF THE PURPLE SHIRT — At the recent opening of the Talent Acquisition Center in the IPOC Building, members of the Talent Acquisition group decided to show their team spirit and unity by wearing matching shirts. Says team member Ken Holley, back row, center, "We represent the pipeline activities — recruiting, advertising, student programs, and represented hiring and testing. We work together to bring the best and brightest candidates for all Sandia employment opportunities. We hope our work and our responsiveness is noticed by all of Sandia." (Photo by Randy Montoya)