

Quality and Productivity Commission
29th Annual Productivity and Quality Awards Program
Champions of Change: Together We Make a Difference

2015 APPLICATION

Title of Project (Limited to 50 characters, including spaces, using Arial 12 point font):

NAME OF PROJECT: DA CYBER INVESTIGATION RESPONSE TEAM

DATE OF IMPLEMENTATION/ADOPTION: JULY 1, 2013
 (Must have been implemented at least one year - on or before July 1, 2014)

PROJECT STATUS: X Ongoing One-time only

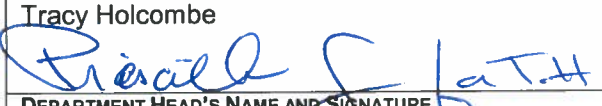
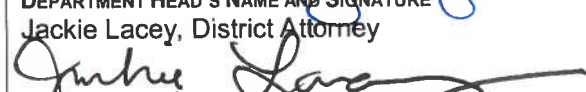
HAS YOUR DEPARTMENT PREVIOUSLY SUBMITTED THIS PROJECT? Yes X No

EXECUTIVE SUMMARY: Describe the project in 15 lines or less using Arial 12 point font. State clearly and concisely what difference the project has made.

1 In the 21st Century, almost every intimate detail of our lives – personal, financial, and
 2 medical – is contained on electronic media. While the County has been able to
 3 successfully use this information technology to improve services for our residents and
 4 employees, this vast trove of data is a constant temptation for hackers and data
 5 thieves. Cyber-attacks can interrupt services, lead to identity theft and fraud,
 6 diminish public trust, and subject the County to enormous civil and regulatory liability.
 7 While the County has a mature and effective cyber incident response protocol, the
 8 evolving threats to our systems, coupled with the burgeoning liability associated with
 9 any data breach, call for innovative approaches. DA-CIRT is a pioneering approach
 10 that contributes the expertise and unique capabilities of the District Attorney's High
 11 Technology Crime Division to the task of defending the County's information assets.
 12 Stopping a cyber-attack before it can infiltrate our systems prevents a single breach;
 13 locating and prosecuting the attacker prevents future attacks by removing that threat,
 14 and deterring others.
 15

(1) ACTUAL/ESTIMATED ANNUAL COST AVOIDANCE	(2) ACTUAL/ESTIMATED ANNUAL COST SAVINGS	(3) ACTUAL/ESTIMATED ANNUAL REVENUE	(1) + (2) + (3) = TOTAL ANNUAL ACTUAL/ESTIMATED BENEFIT	SERVICE ENHANCEMENT PROJECT
\$	\$	\$	\$	<input type="checkbox"/>

ANNUAL = 12 MONTHS ONLY

SUBMITTING DEPARTMENT NAME AND COMPLETE ADDRESS Los Angeles District Attorney's Office		TELEPHONE NUMBER 213-974-3412
PROGRAM MANAGER'S NAME Maria Ramirez, Head Deputy District Attorney		TELEPHONE NUMBER 213-257-2426 EMAIL Maramire@da.lacounty.gov
PRODUCTIVITY MANAGER'S NAME AND SIGNATURE (PLEASE CALL (213) 893-0322 IF YOU DO NOT KNOW YOUR PRODUCTIVITY MANAGER'S NAME) Tracy Holcombe 	DATE 7/15/15	TELEPHONE NUMBER 213-257-2771 EMAIL Tholcombe@da.lacounty.gov
DEPARTMENT HEAD'S NAME AND SIGNATURE Jackie Lacey, District Attorney 	DATE 7/15/15	TELEPHONE NUMBER 213-974-3512

Quality and Productivity Commission
29th Annual Productivity and Quality Awards Program
Champions of Change: Together We Make a Difference

2015 APPLICATION

Title of Project (Limited to 50 characters, including spaces, using Arial 12 point font):

NAME OF PROJECT: DA CYBER INVESTIGATION RESPONSE TEAM

CHALLENGE: In order to deliver services, County agencies must collect and process an enormous amount of information. From where we live and work, the value of our property, our personal medical history, to our bank information, our lives are captured on the County servers. Information and information technology resources are critical to every County function and service, but at the same time, this information is a gold mine to hackers and identity thieves. The challenge is to secure this data from unwanted access, protecting those who trust us with their information and ensuring that County agencies can fulfill their functions and duties.

Breaches in County cyber-security can be devastating, both in human and financial terms. Not only may essential services be interrupted and public confidence in our ability to govern diminished, but criminals may use the stolen information to commit identity theft, often in the form of public benefits fraud. It can take victims years to unravel the mess, and even longer to feel secure. Breaches require victims to be notified and provided credit monitoring services. This financial liability, along with the cost of repairing and securing the system, and potential lawsuits, is significant, diverting limited County resources from other worthy projects.

The potential attack surface for the County's information assets is monumental. The County is directly responsible for critical infrastructures including hospitals, roads, dams, and reservoirs. Its five hospitals treat 800,000 patients a year. The 34 County departments and other governmental units own and manage staggering technical resources including 90,000 workstations, 15,000 laptop computers, 19,000 mobile computers and over 3,000 servers. These systems are under constant cyber-attack from criminals, organized crime groups, terrorist groups, hacktivists and even foreign governments.

The County is well defended by a mature information security program under the direction of the County Chief Information Security Officer and the County incident response process has been nationally recognized as reflecting best practices in information security, yet gaps remained. Staff lacked the ability to determine the origin of attacks or to perform advanced forensic capture and analysis; evidence of cyber-attacks was routinely erased. Despite the hundreds of reported security incidents, no hackers had ever been prosecuted. County information system defenders could benefit from increased access to intelligence about threats to county IT resources and enhanced sharing of this information with the law enforcement and national security communities.

Simply detecting and stopping each attack was insufficient. The County had the resources available to track down these cyber-attackers and bring them to justice; all that was needed was a plan and cooperation.

Quality and Productivity Commission
29th Annual Productivity and Quality Awards Program
Champions of Change: Together We Make a Difference

2015 APPLICATION

Title of Project (Limited to 50 characters, including spaces, using Arial 12 point font):

NAME OF PROJECT: DA CYBER INVESTIGATION RESPONSE TEAM

SOLUTION: In July 2013 the District Attorney created the Cyber Investigation Response Team (DA-CIRT). This team consists of a Deputy District Attorney IV, a Sergeant and four Senior Investigators. These DA-CIRT members are all specially trained and have extensive experience investigating and prosecuting cyber-crime. DA-CIRT works closely with the County's Chief Information Office and the Internal Services Department and is a formal component of the county's cyber incident management plan. DA-CIRT, with sworn law enforcement officers, has capabilities and resources that are simply not available to unsworn County personnel. DA-CIRT members brought with them in excess of \$200,000 worth of training. This figure does not include the training, expertise and investigative resources available to the County through the law enforcement networks brought together by DA-CIRT. DA-CIRT members hold top secret security clearances and often work with the Federal Bureau of Investigation (FBI) and United States Secret Service to respond to attacks originating outside of California or the United States.

When an incident occurs, DA-CIRT is activated and responds immediately, coordinating closely with the Countywide Computer Emergency Response Team (CCERT). Working alongside ISD's information security staff, whose mission it is to secure systems and restore operations, DA-CIRT personnel focus on preserving evidence, identifying those responsible and bringing them to justice.

BENEFITS: DA-CIRT provides both emergency services in response to security incidents and alerts, and ongoing services to strengthen cyber defenses. Since its inception, DA-CIRT has responded to more than 80 incidents involving 24 County departments and over 460,000 exposed personal records, conducting forensic examination and collecting important information about malware attacks that was previously unavailable to CCERT staff.

DA-CIRT investigations have resulted in the successful prosecution of five cases and the filing of felony charges in several pending cases. The persons responsible for the theft of the personal information of nearly 800 County employees, and the subsequent misuse of that information to commit over \$1 million in tax refund fraud have been convicted. The hacker who penetrated a Registrar/Recorder database was convicted and ordered to pay \$30,000.00 in restitution. Still more attackers have been apprehended internationally, including three hackers who placed malware on County systems. Thanks to DA-CIRT, criminal hackers have been ordered to pay more than \$3.9 million in state restitution and \$2.6 million in federal restitution.

DA-CIRT provides unique services on an ongoing basis that strengthen the County's cyber defenses. Our exchange of intelligence about threats and attacks with the FBI, the Secret Service, and the National Cyber Intelligence Joint Task Force enables DA-CIRT to respond to attacks and threats of attacks in a more efficient manner. The sharing of information also significantly increases the likelihood that systems will be protected, and culprits will be identified,

Quality and Productivity Commission
29th Annual Productivity and Quality Awards Program
Champions of Change: Together We Make a Difference

2015 APPLICATION

Title of Project (Limited to 50 characters, including spaces, using Arial 12 point font):

NAME OF PROJECT: DA CYBER INVESTIGATION RESPONSE TEAM

LINKAGE TO THE COUNTY STRATEGIC PLAN (DETAIL IS REQUIRED FOR COUNTY DEPARTMENTS): Use Arial 12 point font

apprehended and brought to justice.

DA-CIRT has identified opportunities to improve existing systems to detect and prevent hacking attacks, including recommending a configuration change to County email systems that has enabled our investigators to review dozens of inbound viruses every week.

Information breaches commonly involve hundreds of thousands of records and at an average cost of \$250 per record, the potential liability is astronomical. An active CIRT team can reduce data breach costs by more than 10 percent and premiums for cyber breach liability insurance decrease when a CIRT team cooperates with law enforcement. DA-CIRT criminal investigations of cyberattacks shortens the length of the investigation, provides quick and accurate assessment of the scope of the data breach, and increases the likelihood of recovering stolen information before it is released then monetized, thereby greatly reducing liability and costs. Criminal prosecution of cyberattacks deters would-be hackers and prevents future data breaches. Penetration and forensic readiness testing improves system security, increases the likelihood and speed of breach detection, and improves our ability to determine the scope of any data loss.

DA-CIRT supports the County's Strategic Plan Goal 1, Operational Effectiveness and Fiscal Sustainability by directly enhancing the effectiveness of County cybersecurity operations and indirectly enhancing the effectiveness of all County operations and the uninterrupted delivery of services. DA-CIRT furthers Strategic Initiative 2: Targeted Risk Management, best risk management practices by limiting data breach liability and the resulting costs. Finally, DA-CIRT enhances Strategic Initiative 4: Innovative Technology Application by protecting the County IT infrastructure and web-based public services and access, thereby minimizing risk and potential liability while enhancing public confidence.

DA-CIRT supports County Strategic Plan Goal 2, Community Support and Responsiveness: Enrich lives of Los Angeles County residents by providing enhanced services, and effectively planning and responding to economic, social, and environmental challenges by providing threat intelligence that enables the County information security framework to effectively plan and respond to cyber-attack challenges. DA-CIRT supports Strategic Initiative 3: Emergency Preparedness by providing training and threat intelligence which expands, and enhances emergency preparedness through continued investment in personnel, training and facilities.

The collaborative efforts of the DA-CIRT emphasize the important role we all play in preventing computer crime and data breaches, promoting a culture of security in which every employee takes responsibility for preventing computer crime.

Quality and Productivity Commission
29th Annual Productivity and Quality Awards Program
Champions of Change: Together We Make a Difference

2015 APPLICATION

Title of Project (Limited to 50 characters, including spaces, using Arial 12 point font):

NAME OF PROJECT: DA CYBER INVESTIGATION RESPONSE TEAM

COST AVOIDANCE, COST SAVINGS, AND REVENUE GENERATED (ESTIMATED BENEFIT): If you are claiming cost benefits, include a calculation on this page. You must include an explanation of the County cost savings, cost avoidance or new revenue that matches the numbers in the box. Remember to keep your supporting documentation. Use Arial 12 point font

Cost Avoidance: Costs that are eliminated or not incurred as a result of program outcomes.

Cost Savings: A reduction or lessening of expenditures as a result of program outcomes.

Revenue: Increases in existing revenue streams or new revenue sources to the County as a result of program outcomes.

(1) ACTUAL/ESTIMATED ANNUAL COST AVOIDANCE	(2) ACTUAL/ESTIMATED ANNUAL COST SAVINGS	(3) ACTUAL/ESTIMATED ANNUAL REVENUE	(1) + (2) + (3) TOTAL ANNUAL ACTUAL/ESTIMATED BENEFIT	SERVICE ENHANCEMENT PROJECT
\$	\$	\$	\$	<input type="checkbox"/>

ANNUAL= 12 MONTHS ONLY

Although a cost savings could not be calculated, as a result of the work done by the DA-CIRT, criminal hackers have been ordered to pay more than \$3.9 million in state restitution and \$2.6 million in federal restitution.

Quality and Productivity Commission
29th Annual Productivity and Quality Awards Program
Champions of Change: Together We Make a Difference

2015 APPLICATION

Title of Project (Limited to 50 characters, including spaces, using Arial 12 point font):

NAME OF PROJECT: DA CYBER INVESTIGATION RESPONSE TEAM

FOR COLLABORATING DEPARTMENTS ONLY

(For single department submissions, do not include this page)

DEPARTMENT NO. 2 NAME AND COMPLETE ADDRESS	
Chief Information Office 350 S. Figueroa, Suite 188 Los Angeles, California 90071	
PRODUCTIVITY MANAGER'S NAME AND SIGNATURE	DEPARTMENT HEAD'S NAME AND SIGNATURE
KIMBERLY JO Signature on file	RICHARD SANCHEZ Signature on file
DEPARTMENT NO. 3 NAME AND COMPLETE ADDRESS	
Internal Services Department 1100 North Eastern Avenue Los Angeles, California 90063	
PRODUCTIVITY MANAGER'S NAME AND SIGNATURE	DEPARTMENT HEAD'S NAME AND SIGNATURE
CELINA ORTIZ Signature on file	DAVID CHITTENDEN Signature on file
DEPARTMENT NO. 4 NAME AND COMPLETE ADDRESS	
PRODUCTIVITY MANAGER'S NAME AND SIGNATURE	DEPARTMENT HEAD'S NAME AND SIGNATURE
DEPARTMENT NO. 5 NAME AND COMPLETE ADDRESS	
PRODUCTIVITY MANAGER'S NAME AND SIGNATURE	DEPARTMENT HEAD'S NAME AND SIGNATURE
DEPARTMENT NO. 6 NAME AND COMPLETE ADDRESS	
PRODUCTIVITY MANAGER'S NAME AND SIGNATURE	DEPARTMENT HEAD'S NAME AND SIGNATURE