eRA, An HHS Grants Solution Provider

Dr. Richard Ikeda, PhD

Director, ORIS

electronic Research Administration (eRA)

Office of Research Information Systems (ORIS)

OER, OD, National Institutes of Health

September 17, 2013

National Institutes of Health

Office of Extramural Research

eRA Program

Supporting the mission-critical function of grants administration for NIH and other federal granting components

eRA operates and maintains 30+ custom-made, large, complex and critical systems that are essential for research done worldwide with grants funded by NIH and eRA's partner agencies
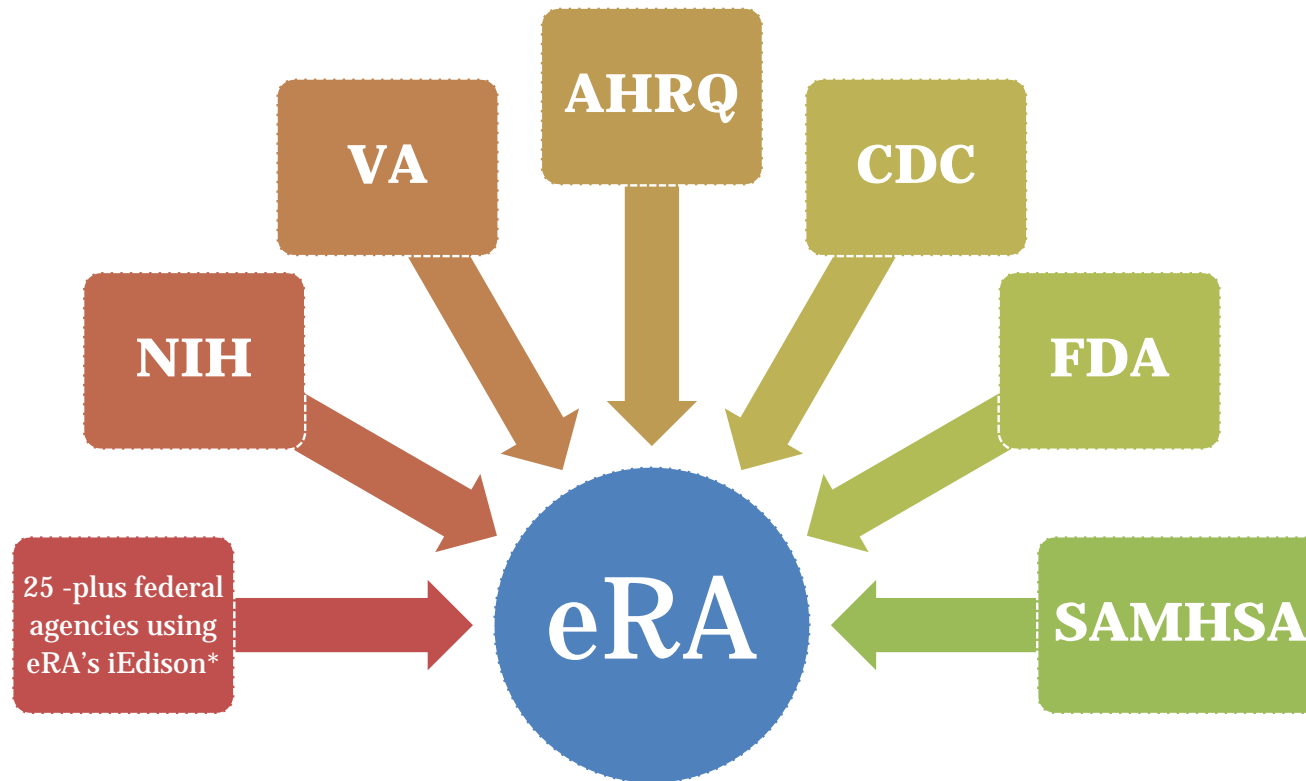
External users: research applicant community, reviewers

Internal users: staff at NIH and eRA's >25 partner agencies

eRA Today: Serving NIH, OpDivs, VA and 25 independent agencies

Currently collaborating with NSF and DoD

eRA By The Numbers
(NIH and eRA's partner agencies)

Total Applications, Awards, Value, (FY2009-12)

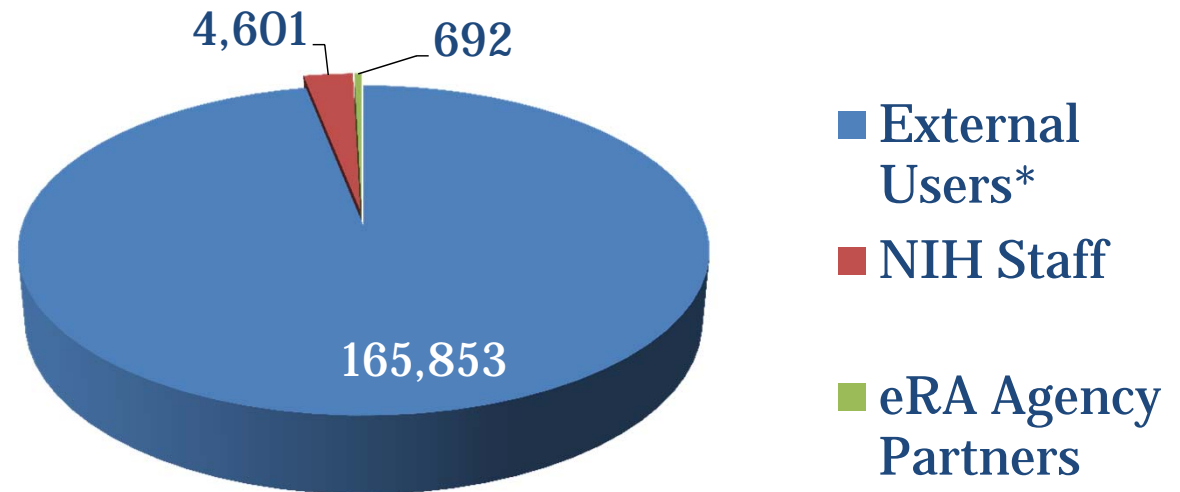| Fiscal Year	Applications received**	Number of Awards**	Current Year Funding**
• FY2012	• 128,746	• 60,902	• $30.34 B
• FY2011	• 127,695	• 60,722	• $29.91 B
• FY2010	• 140,343*	• 69,604*	• $35.36 B
• FY2009	• 151,168*	• 73,671*	• $34.82 B

*Includes ARRA

**Applications and Awards include competing and non-competing applications

47 million database operations a day: individual action(s) by user to select, insert and update data

FY2012 Total Active eRA Users

4,601 692

165,853

- External Users*
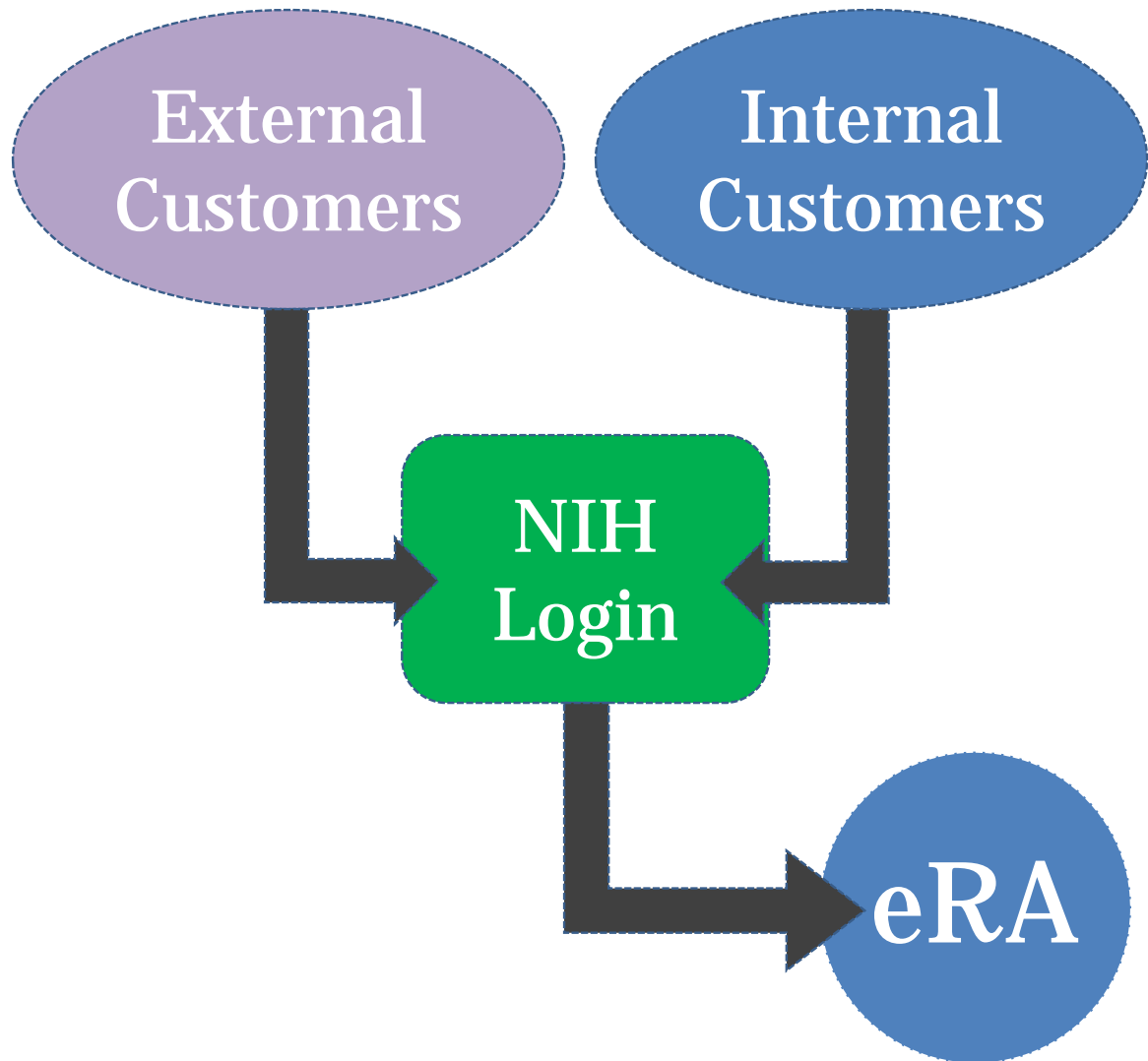- NIH Staff
- eRA Agency Partners

Total active users: **171,146**

Total usage/log-ins: **10.69 million**

Registered research organizations in eRA Commons doubled in the past 5 years to **24,000**

*External users include applicants, grantees and electronic reviewers

eRA and Commons Access

eRA and Commons utilize NIH Login, a single sign-on solution offered by the NIH Center for Information Technology (CIT)

External Customers

Internal Customers

NIH Login

eRA

eRA System Security Categorization

eRA conforms to the NIST FIPS 199 Standards for Security Categorization of Federal Information and Information Systems

Security Objective	POTENTIAL IMPACT		
	LOW (Bronze)	MODERATE (Silver)	HIGH
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Use of InCommon by eRA

InCommon use by eRA has been shown to be practical

- Proof of concept demo for FDP showed that Bronze InCommon credentials can work with NIH Login for access to NIH Commons

- Actual use of InCommon for NIH Commons access will require
  - Silver level certification
  - Work by eRA and CIT (NIH Login) to recognize the metadata that identifies an institution as Silver

- Once InCommon is fully implemented for Silver level access, NIH recognizes that additional capabilities may be required.

Questions?