

---

## Plan Overview

*A Data Management Plan created using DMPTool*

**Title:** Low Temperature Junction Formation for Image Sensors and Charge-Coupled Devices

**Creator:** Jeffrey Kowalski

**Affiliation:** Non Partner Institution

**Funder:** United States Department of Energy (DOE) (energy.gov)

**Funding opportunity number:** 51414

**Grant:** 638278

**Template:** Department of Energy (DOE): Generic

**Last modified:** 05-05-2020

**Grant number / URL:** 638278

**Copyright information:**

The above plan creator(s) have agreed that others may use as much of the text of this plan as they would like in their own plans, and customize it as necessary. You do not need to credit the creator(s) as the source of the language used, but using any of the plan's text does not imply that the creator(s) endorse, or have any relationship to, your project or proposal

# Low Temperature Junction Formation for Image Sensors and Charge-Coupled Devices

---

## Data sharing and preservation

Data management plans should describe whether and how data generated in the course of the proposed research will be [shared](#) and [preserved](#) and, at a minimum, describe how data sharing and preservation will enable [validation](#) of results, or how results could be validated if data are not shared or preserved.

All data generated at DSGI's lab will be available for review by DOE program manager and SLAC support team which is required to validate achieving the projects goals in terms of tool performance. All data is stored on a hard drive on the process tool and will be preserved on DSGI dedicated server. Data will consist of CMOS device performance and wafer uniformity studies. Tool data is collected a a 2 second intervals and is plotted into charts for convenient review and storage

## Data used in publications

Data management plans should provide a plan for making all research data displayed in publications resulting from the proposed research open, machine-readable, and digitally accessible to the public at the time of publication. This includes data that are displayed in charts, figures, images, etc. In addition, the underlying digital research data used to generate the displayed data should be made as accessible as possible to the public in accordance with the [Principles](#) published in the DOE Policy for Digital Research Data Management. The published article should indicate how these data can be accessed.

All collected data will be in a pdf format. Figures and images for potential publications will be in a power point file. The underlying data used to generate these charts are stored on DSGI's dedicated server and will be available to DOE program management.

## Data management resources

Data management plans should consult and reference available information about data management resources to be used in the course of the proposed research. In particular, DMPs that explicitly or implicitly commit data management resources at a facility beyond what is conventionally made available to approved users should be accompanied by written approval from that facility. In determining the resources available for data management at DOE Scientific User Facilities, researchers should consult the [published description of data management resources](#) and practices at that facility and reference it in the DMP.

DSGI has a NDA with SLAC. DSGI has reviewed with SLAC data management resources available for our joint plan research and we understand the approval processes for sharing data.

## Confidentiality, security and rights

Data management plans must protect confidentiality, personal privacy, [Personally Identifiable Information](#) and U.S. national, homeland, and economic security; recognize propriety interests, business confidential information, and intellectual property rights; avoid significant negative impact on innovation and U.S. competitiveness; and otherwise be consistent with all applicable laws, regulations, agreement terms and conditions, and DOE orders and policies.

All employees at DSGI have signed both confidentiality and patent assignment agreements. All employees understand protocol on handling confidential materials through awareness training. All of DSGI confidential material is stored on a dedicated server located at DSGI data room and is backed up on a weekly basis. DSGI data room has limited access and DSGI keeps track of who has the keys and passwords. Cloud applications and file-sharing services are restricted to ensure that company-sanctioned services are properly configured and secured. All third-party systems: IP that is shared with business partners, suppliers, or customers is controlled directly by CEO. All intellectual property and presentation material are labeled clearly with a confidential information banner.